# Gabidulin Codes Achieve List Decoding Capacity with an Order-Optimal Column-To-Row Ratio

**Zeyu Guo**
Department of Computer Science and Engineering, The Ohio State University

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

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

**Zihan Zhang**
Department of Computer Science and Engineering, The Ohio State University

## Abstract

In this paper, we show that random Gabidulin codes of block length $n$ and rate $R$ achieve the (average-radius) list decoding capacity of radius $1 - R - \varepsilon$ in the rank metric with an order-optimal column-to-row ratio of $O(\varepsilon)$. This extends the recent work of Guo, Xing, Yuan, and Zhang (FOCS 2024), improving their column-to-row ratio from $O(\frac{\varepsilon}{n})$ to $O(\varepsilon)$. For completeness, we also establish a matching lower bound on the column-to-row ratio for capacity-achieving Gabidulin codes in the rank metric.

Our proof techniques build on the work of Guo and Zhang (FOCS 2023), who showed that randomly punctured Reed–Solomon codes over fields of quadratic size attain the generalized Singleton bound of Shangguan and Tamo (STOC 2020) in the Hamming metric. The proof of our lower bound follows the method of Alrabiah, Guruswami, and Li (SODA 2024) for codes in the Hamming metric.

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

**Keywords and phrases** coding theory, error-correcting codes, Gabidulin codes, rank-metric codes

**Digital Object Identifier** 10.4230/LIPIcs.APPROX/RANDOM.2025.43

**Category** RANDOM

**Funding** *Zeyu Guo*: Supported by NSF grant CCF-2440926.
*Zihan Zhang*: Supported by NSF grant CCF-2440926.

**Acknowledgements** The authors thank the anonymous RANDOM 2025 reviewers for their helpful comments.

## 1 Introduction

Introduced by Delsarte [5], rank-metric codes have since developed into a field of study with applications and connections spanning network coding [16, 26, 17, 25], space-time coding [21, 20], cryptography [10, 9, 18, 19], and pseudorandomness [7, 6, 15, 14, 11].

A rank-metric code is a collection of matrices in $\mathbb{F}_q^{m\times n}$ with $m \geq n$, where the distance between two matrices $A$ and $B$ is defined to be their *rank distance* $\operatorname{rank}(A-B)$. A rank-metric code $C \subseteq \mathbb{F}_q^{m\times n}$ of rate $R := \frac{\log_2 |C|}{\log_2(q^{mn})}$ and relative minimum (rank) distance $\delta$ must satisfy that $R + \delta \leq 1$, which is called the Singleton bound. A rank-metric code attaining the Singleton bound is called a maximum rank distance (MRD) code. Gabidulin codes are an important class of MRD codes, which can be seen as the linearized version of Reed–Solomon codes. This analogy allows us to design efficient encoding and unique decoding algorithms for Gabidulin codes. However, when it comes to the list decoding regime, it is known that some Gabidulin codes are not list decodable beyond the unique decoding radius [22, 23].

Thus, it is impossible to design a list decoding algorithm for all Gabidulin codes. Moreover, it was not even clear if any Gabidulin codes were list decodable beyond the unique decoding radius until very recently. Guo, Xing, Yuan and Zhang [12] recently proved that random Gabidulin codes are not only list decodable beyond the unique decoding radius but also attain the optimal *generalized Singleton bound* (see Lemma 1) with high probability. This settles an open problem of whether there exist list decodable Gabidulin codes.

However, the construction in [12] requires $m$, the number of rows of matrices, to be at least quadratic in $n$, so the column-to-row ratio $\frac{n}{m} = O(\frac{1}{n})$ tends to zero as $n$ grows. This is analogous to a result of Brakensiek, Gopi, and Makam on Reed–Solomon codes [4], which states that any Reed–Solomon code exactly attaining the generalized Singleton bound must have an exponential field size. Suppose the list decoding radius is slightly off the generalized Singleton bound (with a gap of $\varepsilon$). In that case, Guo and Zhang [13] proved that the field size of Reed–Solomon codes can be brought down to quadratic which was further brought down to linear in the follow-up work of Alrabiah, Guruswami, and Li [2].

Thus, this raises an open problem for rank-metric codes, already asked in [12]: Can we obtain a similar result for Gabidulin codes as well?

▶ **Open Problem 1.** *Do there exist Gabidulin codes of constant column-to-row ratio that are list decodable in the rank metric?*

In this paper, we provide a positive answer to this open problem. We show that if the list decoding radius is slightly off the generalized Singleton bound (with a gap of $\varepsilon$), then a random Gabidulin code $C \subseteq \mathbb{F}_q^{m\times n}$ with $m = O(\frac{n}{\varepsilon})$ is list decodable up to this bound with high probability. Moreover, we complement our positive result by proving an upper bound $m = \Omega(\frac{n}{\varepsilon})$ for any list decodable Gabidulin codes approaching the generalized Singleton bound with a gap of $\varepsilon$. One can find the details in the following subsection.

## 1.1 Main Results

In this paper, we mainly focus on the rank distance, which is defined to be the rank of the difference between two matrices $A, B \in \mathbb{F}_q^{m\times n}$ i.e., $d(A, B) := \mathrm{rank}(A - B)$. In what follows, $d(\cdot, \cdot)$ refers to the rank distance. For $\rho \in [0, 1]$, a code $C \subseteq \Sigma^n$ over an alphabet $\Sigma$ is said to be $(\rho, \ell)$-*list decodable* if for any $\boldsymbol{y} \in \mathbb{F}_q^n$, it holds that

$$|\{\boldsymbol{x} \in C : d(\boldsymbol{x}, \boldsymbol{y}) \le \rho n\}| \le \ell,$$

where $d(\boldsymbol{x}, \boldsymbol{y})$ denotes the distance between $\boldsymbol{x}$ and $\boldsymbol{y}$. Here, $\rho$ is called the list decoding radius, and $\ell$ is called the list size. The stronger notion of $(\rho, \ell)$-*average-radius list decodability* is defined in the same way, except that we replace the maximum of the distances $d(\boldsymbol{c}_i, \boldsymbol{y})$ by the average of these distances. The formal definition is given as follows.

▶ **Definition 2** (Average-radius list decodability)**.** A code $C \subseteq \Sigma^n$ is $(\rho, \ell)$ average-radius list decodable if for any $\boldsymbol{y} \in \Sigma^n$ and $\ell + 1$ distinct codewords $\boldsymbol{c}_0, \boldsymbol{c}_1, \dots, \boldsymbol{c}_\ell \in C$, it holds that

$$\frac{1}{\ell+1}\sum_{i=0}^{\ell} d(\boldsymbol{y}, \boldsymbol{c}_i) > \rho n.$$

In [24], Shangguan and Tamo proved the *generalized Singleton bound* for list decoding, generalizing the classical Singleton bound for unique decoding. For linear codes, this generalized Singleton bound states that if $C \subseteq \mathbb{F}_q^n$ is an $[n, k]$-linear code that is $(\rho, \ell)$-list decodable in the Hamming metric, then it holds that $\rho \le \frac{\ell}{\ell+1}\left(1 - \frac{k}{n}\right)$. In [12], they noted that this generalized Singleton bound also holds for rank-metric codes.

▶ **Lemma 1** (Generalized Singleton bound for rank-metric codes [12, Lemma 2.1]). *Let $C \subseteq \mathbb{F}_{q^m}^n$ be an $[n,k]_{\mathbb{F}_{q^m}}$-linear code that is $(\rho,\ell)$-list decodable in the rank metric. Then it holds that*

$$\rho \le \frac{\ell}{\ell+1}\left(1-\frac{k}{n}\right).$$

They further showed that this bound is tight for rank-metric codes by proving that random Gabidulin codes attain it with high probability. (This is a nontrivial task; in fact, even proving that random linear rank-metric codes attain the generalized Singleton bound is far from obvious.) However, the column-to-row ratio of these codes is quite small, which makes them less appealing for practical applications.

▶ **Theorem 3** ([12, Lemma 1.3]). *Let $(\alpha_1,\dots,\alpha_n)$ be uniformly distributed over the set of all vectors in $\mathbb{F}_{q^m}^n$ whose coordinates are linearly independent over $\mathbb{F}_q$. Suppose $m \ge cnk\ell + \log_q(1/\delta)$, where $c$ is a large enough absolute constant. Then it holds with probability at least $1-\delta$ that the Gabidulin code $\mathcal{G}_{n,k}(\alpha_1,\dots,\alpha_n)$[1] over $\mathbb{F}_{q^m}$ is $\left(\frac{L}{L+1}\left(1-k/n\right), L\right)$-list decodable for all $L \in [\ell]$ in the rank metric.*

In this paper, we prove that there exist Gabidulin codes with constant column-to-row ratio $\Omega(\varepsilon)$ that are list decodable up to the radius $\frac{\ell}{\ell+1}(1-\frac{k}{n}-\varepsilon)$.

▶ **Theorem 4.** *Let $\varepsilon > 0$ and $n,k$ be positive integers with $k \le n$. Let $m$ and $\ell$ be positive integers such that $m \ge \frac{c\ell(\ell+1)n}{\varepsilon}$, where $c$ is a sufficiently large absolute constant. Then with probability at least $1-q^{-O(n)} > 0$, a random Gabidulin code of rate $R = k/n$ and block length $n$ over $\mathbb{F}_{q^m}^n$ is $\left(\frac{\ell}{\ell+1}(1-R-\varepsilon),\ell\right)$ average-radius list decodable.*

Complementing this result, we also show that the column-to-row ratio is at most $O(\varepsilon)$ for any rank-metric code that is average-radius list decodable up to the generalized Singleton bound. Thus, our results are essentially tight.

▶ **Theorem 5.** *Let $\ell \ge 2$. For any $R \in [0,1]$, any rank-metric code $C \subseteq \mathbb{F}_{q^m}^n$ of rate $R$ that is $\left(\frac{\ell(1-R-\varepsilon)}{\ell+1},\ell\right)$-average-radius list decodable must have $m = \Omega\left(\frac{Rn}{\varepsilon}\right)$.*

## 1.2 Proof Overview

Our proof is inspired by [13]. To explain our proof, we first briefly review the techniques in [13]. In [13], they proposed the notion of a reduced intersection matrix, whose kernel corresponds to the list of codewords. Let $C$ be an $[n,k]$ linear code and $G$ be its generator matrix, which is a $k \times n$ matrix. Given $\ell+1$ distinct codewords $\boldsymbol{c}_1,\dots,\boldsymbol{c}_{\ell+1}$ with $\boldsymbol{c}_i = \boldsymbol{x}_i G = (c_{i1},\dots,c_{in})$ that are close to a vector $\boldsymbol{y} = (y_1,\dots,y_n)$, where the coordinates $c_{ij}$ and $y_j$ are in the alphabet $\mathbb{F}$, we define the intersection index set $I_j := \{h \in [n] : y_h = c_{jh}\}$. For a subset $J \subseteq [n]$, let $G_J$ (resp. $\boldsymbol{y}_J$) be the submatrix (resp. subvector) of $G$ (resp. $\boldsymbol{y}$) formed by the columns (resp. components) with indices in $J$. Then, we have $\boldsymbol{y}_{I_i} - \boldsymbol{x}_i G_{I_i} = 0$. If $a \in I_i \cap I_j$, then $(\boldsymbol{x}_i - \boldsymbol{x}_j)G_a = 0$. This means that for each element in $I_i \cap I_j$, we can establish a linear equation. Since these $\ell+1$ codewords are very close to $\boldsymbol{y}$, it is expected that we can obtain many equations of the form $(\boldsymbol{x}_i - \boldsymbol{x}_j)G_a = 0$. By removing the linear dependence of these equations, we obtain a reduced intersection matrix $R_{G,I_{[\ell]}}$ such that $(\boldsymbol{x}_2 - \boldsymbol{x}_1,\dots,\boldsymbol{x}_{\ell+1} - \boldsymbol{x}_1)R_{G,I_{[\ell]}} = 0$, where $I_{[\ell]}$ is a shorthand for the tuple $(I_1,\dots,I_n)$. On

[1] See the definition of Gabidulin codes in Definition 13.

the other hand, if $R_{G,I_{[\ell]}}$ has full rank, then we cannot find $\ell+1$ distinct codewords that are close to a vector $\boldsymbol{y}$ and thus $C$ is list decodable. Thus, the essence of their paper is to investigate the full rankness of $R_{G,I_{[\ell]}}$.

In this paper, we investigate the list decodability of rank-metric codes, where distance is measured using the rank metric rather than the Hamming metric. Thus, we cannot construct the reduced intersection matrix $R_{G,I_{[\ell]}}$ row by row as in [13]. Instead, we present another construction of a reduced intersection matrix, which captures the property of the rank distance. Let us first represent the codeword of our rank-metric code as a vector $\boldsymbol{c} \in \mathbb{F}^n$ where $\mathbb{F}$ is the extension field of $\mathbb{F}_q$. This is done by fixing an $\mathbb{F}_q$-linear isomorphism $\mathbb{F} \cong \mathbb{F}_q^{[\mathbb{F}:\mathbb{F}_q]}$. The rank distance between two codewords $d(\boldsymbol{c}_1, \boldsymbol{c}_2)$ is the maximum number of $\mathbb{F}_q$-linear independent components in $\boldsymbol{c}_1 - \boldsymbol{c}_2$. One can find the precise definition in Section 2. Similar to Hamming codes, a linear rank-metric code has a generator matrix $G$ and each codeword can be encoded as $\boldsymbol{c} = \boldsymbol{x}G$. Given two vectors $\boldsymbol{y}_1, \boldsymbol{y}_2 \in \mathbb{F}^n$ with rank distance $d$, we can find a $(n-d) \times n$ matrix $A$ over $\mathbb{F}_q$ of full rank such that $A(\boldsymbol{y}_1 - \boldsymbol{y}_2)^\top = 0$. The major difference between the rank metric and the Hamming metric is that for each vector $\boldsymbol{v}$ that lies in the vector space spanned by the rows in $A$, we always have $\boldsymbol{v}(\boldsymbol{y}_1 - \boldsymbol{y}_2)^\top = 0$. Thus, we cannot include all $\boldsymbol{v}$ in our equations. Instead, we include $A$ as a whole.

With this observation in mind, we present our new reduced intersection matrix. Assume distinct codewords $\boldsymbol{c}_1, \ldots, \boldsymbol{c}_{\ell+1}$ with $\boldsymbol{c}_i = \boldsymbol{x}_i G$ are close to a vector $\boldsymbol{y} = (y_1, \ldots, y_n)$. Assume that $d(\boldsymbol{y}, \boldsymbol{x}_i G) = a_i$ and there exists an $a_i \times n$ matrix $A_i$ of full rank over $\mathbb{F}_q$ such that $A_i(\boldsymbol{y} - \boldsymbol{x}_i G)^\top = 0$. By replacing $\boldsymbol{y}$ with $\boldsymbol{y} - \boldsymbol{x}_1 G$ and $\boldsymbol{x}_i = \boldsymbol{x}_i - \boldsymbol{x}_1$, we have $A_1 \boldsymbol{y}^\top = 0$ and $A_i(\boldsymbol{y} - \boldsymbol{x}_i G)^\top = 0$. Let $\mathcal{V} = (V_1, \ldots, V_{\ell+1})$ where $V_i$ is the vector space spanned by the rows in $A_i$.[2] Then, we construct a reduced intersection matrix $R_{G,\mathcal{V}}$ to represent all these relations as $R_{G,\mathcal{V}}(\boldsymbol{y}, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_{\ell+1})^\top = 0$ which can be found in (9). If $R_{G,\mathcal{V}}$ has full rank, which means that we cannot find such $\ell+1$ distinct codewords, then our rank-metric code is list decodable. Thus, it suffices to study the rank of $R_{G,\mathcal{V}}$. If our decoding radius is slightly off the generalized Singleton bound (with a gap of $\varepsilon$), then $R_{G,\mathcal{V}}$ is not square. This makes the full rank condition easier to meet.

We restrict $G$ to a subspace $V$ by defining $G_V$ to be the column space of $GA$ where the columns of $A$ span $V$. This can be seen as a generalization of puncturing in the Hamming metric. By introducing a subspace $V$, we obtain a submatrix $R_{G,\mathcal{V}}^V$ of $R_{G,\mathcal{V}}$ by restricting $G$ to $V$. Using results from [12], we show that if $G$ is a symbolic Gabidulin code (see Definition 15), then the submatrix $R_{G,\mathcal{V}}^V$ is invertible and has the same rank as $R_{G,\mathcal{V}}$ when the dimension of $V$ is not too small, i.e., $\dim(V) \geq n - \frac{\lambda k}{\ell}$, where $\lambda > 0$ is a small parameter depending on $\varepsilon$. This means if each variable of this symbolic Gabidulin code is chosen uniformly at random, with high probability, $R_{G,\mathcal{V}}^V$ has full rank. To show that a Gabidulin code is list decodable, we need to enumerate all possible $t$-tuples $(V_1, \ldots, V_t)$ for $t = 1, \ldots, \ell+1$ and take a union bound over all these tuples. Thus, we need to show that $R_{G,\mathcal{V}}$ is of full rank with high probability $1 - \exp(\Omega(-n^2))$ for each $\mathcal{V}$. To do this, we borrow the idea of [13] to bound the failure probability.

Let us briefly review the idea of our algorithm. Let $\boldsymbol{e}_1, \ldots, \boldsymbol{e}_n$ be a standard basis of $\mathbb{F}_q^n$. We first fix a non-singular maximal square submatrix $W$ of $R_{G,\mathcal{V}}$. The reason we need a square submatrix is that it is easy to calculate the determinant of $W$ to bound the failure probability that $W$ is non-singular. Initially, since $G$ is the generator matrix of a symbolic Gabidulin code, $W$ is a nonsingular matrix. If $W$ remains non-singular with the

[2] In our analysis, we need to consider $\mathcal{V}_{[t]} = (V_1, \ldots, V_t)$ for $t = 1, \ldots, \ell+1$. Here, we only consider $\mathcal{V}_{[\ell+1]}$ for simplicity.

assignment $X_1 = \alpha_1, \dots, X_n = \alpha_n$, we are done. Otherwise, we face the situation where $M$ is non-singular under the partial assignment $X_1 = \alpha_1, \dots, X_{j-1} = \alpha_{j-1}$ but becomes singular under $X_1 = \alpha_1, \dots, X_j = \alpha_j$. In this case, we call $j$ a *faulty index* and remove the corresponding columns from the generator matrix $G$. Then, we come to the submatrix $R^V_{G,\mathcal{V}}$ for some subspace $V = \text{span}\{\boldsymbol{e}_i : i \in [n]/\{j\}\}$. Note that we have already shown that $R^V_{G,\mathcal{V}}$ has full rank if $V$ has large dimension. Then, we find a new maximal square submatrix $W$ of $R^V_{G,\mathcal{V}}$ and continue the argument. We show that, with high probability, there are not too many faulty indices, which implies that we can finally find a maximal square submatrix $W$ that has full rank under the assignment. This means $R_{G,\mathcal{V}}$ has full rank, completing the proof.

Complementing our positive result, we also show that a capacity-achieving list decodable rank-metric code must satisfy $m = \Omega(n/\varepsilon)$. Our proof generalizes the proof in [1] in the rank-metric case. In particular, we first fix a subspace $V_0 \subseteq \mathbb{F}^n_{q^m}$ of dimension $b = 4\varepsilon n$ and let $\overline{V}_0$ be a complement of $V_0$. Then, we construct a collection $\mathcal{F}$ of subspaces of dimension $R - \varepsilon$ in $\overline{V}_0$, where $R$ is the rate of our rank-metric code. For any two subspaces $V_1, V_2 \in \mathcal{F}$, $\dim(V_1 + V_2) \geq (R + \varepsilon)n$. We manage to show that $\mathcal{F}$ has a large size. Using a probabilistic argument, we find a codeword $M$ in the rank-metric code $C$ such that for most subspaces $V \in \mathcal{F}$, there is a corresponding codeword $M_V$ in $C$ satisfying the condition that the kernel of $M - M_V$ contains $V$. Since the number of such subspaces is greater than $\ell q^{4\varepsilon n}$, by the pigeonhole principle, we can find $\ell$ distinct codewords $M_{V_1}, \dots M_{V_\ell}$ such that the kernel of $M - M_{V_i}$ also contains $V_0$. Then, we show that these $\ell + 1$ codewords $M, M_{V_1}, \dots M_{V_\ell}$ are contained in a ball of small radius in the rank metric. This implies an upper bound on the list decoding radius, thus completing the proof.

▶ Remark. It is interesting to note that we require only the ideas from [13] to improve the column-to-row ratio to $\Omega_{\ell,\varepsilon}(1)$, without relying on the more refined techniques from [2]. This is likely due to the significantly larger alphabet size of rank-metric codes. While the techniques in [2] might further improve lower-order factors, such as the dependence on $\ell$, we do not pursue this direction here in order to keep the presentation simple.

## 2 Preliminaries

In this paper, vectors are considered row vectors unless stated otherwise. Define $[k] = \{1, \dots, k\}$. Let $\mathbb{F}_q$ be a finite field with $q$ elements and $\mathbb{F}/\mathbb{F}_q$ be a (finite or infinite) extension of $\mathbb{F}_q$.

### 2.1 Vector Spaces

$\mathbb{F}^n_q$ is a vector space of dimension $n$ over $\mathbb{F}_q$. We denote by $\boldsymbol{x}$ a row vector in $\mathbb{F}^n_q$ and $\boldsymbol{x}^\top$ a column vector. Let $\boldsymbol{e}_1, \dots, \boldsymbol{e}_n$ be the standard basis of $\mathbb{F}^n_q$. Given a matrix $A \in \mathbb{F}^{m \times n}_q$, we denote by $\langle A \rangle$ the subspace spanned by the column vectors in $A$. For a $t$-tuple $\mathcal{V}_{[t]} = (V_1, \dots, V_t)$ and $J \subseteq [t]$, define $\mathcal{V}_J = (V_i)_{i \in J}$.

▶ **Definition 6** (Dual space). Let $V \subseteq \mathbb{F}^n_q$ be a linear subspace. The dual space of $V_i$ is denoted as $V^\perp = \{\boldsymbol{v} \in \mathbb{F}^n_q : \boldsymbol{v}\boldsymbol{x}^\top = 0, \quad \forall \boldsymbol{x} \in V\}$. It is clear that $V^\perp$ is well-defined, and $\dim(V^\perp) = n - \dim(V)$.

#### 2.1.0.1 Linear codes.

Let $\mathbb{F}$ be a field. An $[n,k]_\mathbb{F}$ *linear code* $C$ (or $[n,k]_\mathbb{F}$ *code* for short) is simply a subspace of $\mathbb{F}^n$ of dimension $k$. The *dual code* of an $[n,k]_\mathbb{F}$ code $C$ is the $[n, n-k]_\mathbb{F}$ code $C^\perp$ which is the dual space of $C$.

For an $[n,k]_{\mathbb{F}}$ code $C$, a matrix $G \in \mathbb{F}^{k\times n}$ is said to be a *generator matrix* of $C$ if $C = \{\boldsymbol{u}G : u \in \mathbb{F}^k\}$, and a matrix $H \in \mathbb{F}^{(n-k)\times n}$ is said to be a *parity-check matrix* of $C$ if $C = \{\boldsymbol{v} \in \mathbb{F}^n : H\boldsymbol{v}^\top = 0\}$. A generator matrix of $C$ is also a parity-check matrix of the dual code $C^\perp$. Similarly, a parity-check matrix of $C$ is also a generator matrix of $C^\perp$.

▶ **Definition 7** (Dimension of a collection of vector spaces)**.** For a $t$-tuple $\mathcal{V}_{[t]} = (V_1, \ldots, V_t)$ of subspaces and $J \subseteq [t]$, the dimension of $\mathcal{V}_J$ is defined as

$$\dim(\mathcal{V}_J) := \sum_{i\in J} \dim(V_i) - \dim\left(\sum_{i\in J} V_i\right).$$

We need the following simple lemmas, whose proofs are omitted.

▶ **Lemma 2.** *Let $\ell \leq n$. Let $T_1$ be a $\ell\times n$ matrix of full rank over $\mathbb{F}$. Then there exist matrices $M_1 \in \mathbb{F}^{n\times\ell}$, $M_2 \in \mathbb{F}^{n\times(n-\ell)}$, and $T_2 \in \mathbb{F}^{(n-\ell)\times n}$ of full rank such that $M_1T_1 + M_2T_2 = I_n$ and $T_1M_2 = 0$.*

▶ **Lemma 3.** *Let $V_1, \ldots, V_\ell \subseteq \mathbb{F}^n$. Then*

$$\left(\bigcap_{i=1}^{\ell} V_i\right)^{\perp} = \sum_{i=1}^{\ell} V_i^{\perp}. \tag{1}$$

▶ **Lemma 4.** *Let $V$ be a subspace in $\mathbb{F}_q^n$ and $W$ be a subspace of $V$. Then, there exists a matrix $A \in \mathbb{F}_q^{n\times\dim(V)}$ with $\langle A\rangle = V$ such that there exists a $n \times \dim(W)$ submatrix $B$ of $A$ with $\langle B\rangle = W$.*

▶ **Lemma 5.** *Let $0 < \alpha < \beta < 1$ with $\beta - \alpha < \frac{1}{4}$. Given a subspace $V_1 \subseteq \mathbb{F}_q^n$ of dimension $\alpha n$, the number of $V_2 \subseteq \mathbb{F}_q^n$ with $\dim(V_1 + V_2) \leq \beta n$ and $\dim(V_2) = \alpha n$ is at most $16n^2q^{(\beta-\alpha)(1+3\alpha-2\beta)n^2}$.*

**Proof.** Let $W = V_1 \cap V_2$ and we write $V_1 = W \oplus W_1$ and $V_2 = W \oplus W_2$. Since

$$\dim(V_1 \cap V_2) = \dim(V_1) + \dim(V_2) - \dim(V_1 + V_2) \geq (2\alpha - \beta)n,$$

we conclude that $a := \dim(W) \geq (2\alpha-\beta)n$ and $b := \dim(W_2) \leq (\beta-\alpha)n$. To construct $V_2$, it suffices to construct $W$ and $W_2$ separately. The number of subspaces $W$ equals the number of ways of picking a $\dim(W)$-dimensional subspace from $V_1$, which is at most $4q^{(\alpha n-a)a}$. On the other hand, the number of $W_2$ equals the number of ways of picking a $\dim(W_2)$-dimensional subspace that $W_2 \cap V_1 = \{0\}$, which is

$$\prod_{i=0}^{\dim(W_2)-1} \frac{q^n - q^{\alpha n+i}}{q^{\dim(W_2)} - q^i} \leq 4q^{(n-b)b}.$$

Thus, for fixed $(a, b)$, the total number of $V_2$ is at most $16q^{(\alpha n-a)a+(n-b)b}$ subject to $a+b = \alpha n$ and $b \leq (\beta - \alpha)n$. And we have

$$(\alpha n - a)a + (n - b)b = b(\alpha n - b) + (n - b)b = b((\alpha + 1)n - 2b) \leq (\beta - \alpha)(1 + 3\alpha - 2\beta)n^2.$$

The number of possible $(a, b)$ is at most $n^2$. The claim follows by taking the union bound over all possible $(a, b)$. ◀

▶ **Corollary 8.** *Let $0 < \alpha < \beta < 1$. There exists a collection $\mathcal{F}$ of $\alpha n$-dimensional subspaces in $\mathbb{F}_q^n$ of size at least $\Omega(q^{(\alpha-\alpha^2-2(\beta-\alpha)-o(1))n^2})$ such that for any $V_1, V_2 \in \mathcal{F}$, $\dim(V_1+V_2) \geq \beta n$.*

**Proof.** There are at least $q^{\alpha(1-\alpha)n^2}$ $\alpha n$-dimensional subspaces in $\mathbb{F}_q^n$. For each such subspace $V$, by Lemma 5, we remove at most $16n^2 q^{(\beta-\alpha)(1+3\alpha-2\beta)n^2}$ subspaces $W$ in $\mathbb{F}_q^n$ such that $\dim(V+W) \leq \beta n$. Thus, by a greedy algorithm (i.e., iteratively adding subspaces that have not been selected or removed to $\mathcal{F}$), we can find $\mathcal{F}$ of size at least

$$\frac{1}{16n^2} q^{\alpha(1-\alpha)n^2-(\beta-\alpha)(1+3\alpha-2\beta)n^2} \geq \Omega(q^{(\alpha-\alpha^2-2(\beta-\alpha)-o(1))n^2}).$$

The last inequality is due to $1+3\alpha-2\beta \leq 1+\alpha \leq 2$. The proof is completed. ◀

The size of family $\mathcal{F}$ will be used in the lower bound argument in Appendix A.

## 2.2 Rank-Metric Codes

We first review some basic facts and results about rank-metric codes. The *rank distance* $d(A, B)$ between two matrices $A, B \in \mathbb{F}_q^{m\times n}$ is defined to be the rank of $A - B$, i.e., $d(A,B) := \mathrm{rank}(A-B)$. Indeed, this defines a distance [8]. A rank-metric code $C$ is a subset of $\mathbb{F}_q^{m\times n}$ whose rate and minimum distance are given by

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

Without loss of generality, we always assume that $m \geq n$, since otherwise we can exchange $n$ and $m$. It is convenient to treat an $m \times n$ matrix $A$ over $\mathbb{F}_q$ as a vector $\boldsymbol{v} = (v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n$ by identifying $\mathbb{F}_q^m$ with $\mathbb{F}_{q^m}$ (by fixing a basis of $\mathbb{F}_{q^m}$) and viewing each column of $A$ as an element in $\mathbb{F}_{q^m}$. Then, we have $\mathrm{rank}(A) = \dim_{\mathbb{F}_q}(\mathrm{span}_{\mathbb{F}_q}\{v_1, \ldots, v_n\})$. In this way, a rank-metric code $C$ may be viewed as a subset of $\mathbb{F}_{q^m}^n$, and we can study linear rank-metric codes, i.e, codes that are $\mathbb{F}_{q^m}$-subspaces.

#### 2.2.0.1 Linear rank-metric codes over a general field $\mathbb{F}/\mathbb{F}_q$.

It is convenient for us to consider a general notion of linear rank-metric codes $C \subseteq \mathbb{F}^n$ over a field $\mathbb{F}/\mathbb{F}_q$ that can even be infinite. To properly define this notion, we first define the $\mathbb{F}_q$-rank and the kernel subspace of a vector $\boldsymbol{v} \in \mathbb{F}^n$.

▶ **Definition 9** ($\mathbb{F}_q$-rank)**.** Let $\mathbb{F}$ be an extension field of $\mathbb{F}_q$. For $\boldsymbol{v} = (v_1, \ldots, v_n) \in \mathbb{F}^n$, define

$$\mathrm{rank}_{\mathbb{F}_q}(\boldsymbol{v}) := \dim_{\mathbb{F}_q}(\mathrm{span}_{\mathbb{F}_q}\{v_1, \ldots, v_n\}),$$

called the $\mathbb{F}_q$-*rank* of $\boldsymbol{v}$.

▶ **Definition 10** (Kernel subspace)**.** For $\boldsymbol{v} = (v_1, \ldots, v_n) \in \mathbb{F}^n$, define the $\mathbb{F}_q$-*kernel subspace* (or simply the *kernel subspace*) of $\boldsymbol{v}$ to be

$$\ker_{\mathbb{F}_q}(\boldsymbol{v}) := \left\{\boldsymbol{u} \in \mathbb{F}_q^n : \boldsymbol{u}\boldsymbol{v}^\top = 0\right\} = \left\{(u_1, \ldots, u_n) \in \mathbb{F}_q^n : \sum_{i=1}^n u_i v_i = 0\right\}.$$

The following lemma can be seen as an alternative definition of the $\mathbb{F}_q$-rank.

▶ **Lemma 6.** $\mathrm{rank}_{\mathbb{F}_q}(\boldsymbol{v}) = n - \dim_{\mathbb{F}_q}(\ker_{\mathbb{F}_q}(\boldsymbol{v}))$.

**Proof.** Consider the $\mathbb{F}_q$-linear map $\mathbb{F}_q^n \to \mathbb{F}$ sending $\boldsymbol{u} \in \mathbb{F}_q^n$ to $\boldsymbol{u}\boldsymbol{v}^\top$. The image of this map is $\operatorname{span}_{\mathbb{F}_q}\{v_1, \ldots, v_n\}$, whose dimension is $\operatorname{rank}_{\mathbb{F}_q}(\boldsymbol{v})$ by definition. The kernel of this map is $\ker_{\mathbb{F}_q}(\boldsymbol{v})$. So $\operatorname{rank}_{\mathbb{F}_q}(\boldsymbol{v}) = n - \dim_{\mathbb{F}_q}(\ker_{\mathbb{F}_q}(\boldsymbol{v}))$. ◀

We can now define the notion of a linear rank-metric code over a field $\mathbb{F}/\mathbb{F}_q$.

▶ **Definition 11** (Linear rank-metric code)**.** Let $\mathbb{F}$ be an extension field of $\mathbb{F}_q$. An $[n,k]_\mathbb{F}$ (*linear*) *rank-metric code* is simply an $[n,k]_\mathbb{F}$ code $C \subseteq \mathbb{F}^n$ equipped with the distance function $d : \mathbb{F}^n \times \mathbb{F}^n \to \mathbb{N}$ defined by $d(\boldsymbol{v}, \boldsymbol{v}') := \operatorname{rank}_{\mathbb{F}_q}(\boldsymbol{v} - \boldsymbol{v}')$. The *minimum distance* of $C$ is

$$d(C) := \min_{\substack{\boldsymbol{v},\boldsymbol{v}' \in C \\ \boldsymbol{v} \neq \boldsymbol{v}'}} d(\boldsymbol{v}, \boldsymbol{v}') = \min_{\boldsymbol{0} \neq \boldsymbol{v} \in C} \operatorname{rank}_{\mathbb{F}_q}(\boldsymbol{v}).$$

Analogous to the classical setting, one can prove the following Singleton bound for linear rank-metric codes. While this may be well known, we include a proof for completeness.

▶ **Theorem 12** (Singleton bound)**.** *Let $C$ be an $[n,k]_\mathbb{F}$ rank-metric code. Then $d(C) \leq n - k + 1$.*[3]

**Proof.** There exists a nonzero codeword $\boldsymbol{v} = (v_1, \ldots, v_n) \in C$ whose first $k-1$ coordinates are zero. So $d(C) \leq \operatorname{rank}_{\mathbb{F}_q}(\boldsymbol{v}) = \dim_{\mathbb{F}_q}(\operatorname{span}_{\mathbb{F}_q}\{v_1, \ldots, v_n\}) = \dim_{\mathbb{F}_q}(\operatorname{span}_{\mathbb{F}_q}\{v_k, \ldots, v_n\}) \leq n - k + 1$. ◀

A rank-metric code meeting the Singleton bound is called maximum rank distance (MRD) code.

▶ **Lemma 7** ([12, Lemma 2.11])**.** *Let $C$ be an $[n,k]_\mathbb{F}$ code. If $C$ is* MRD*, then $C^\perp$ is also* MRD.

▶ **Lemma 8.** *Let $G \in \mathbb{F}^{k \times n}$ be a generator matrix of an $[n,k]_\mathbb{F}$ code $C$ and $H \in \mathbb{F}^{(n-k) \times n}$ be a parity-check matrix of code $C$. Then the following are all equivalent:*

1. *$C$ is* MRD.
2. *For any $A \in \mathbb{F}_q^{n \times k}$ of full rank, the matrix $GA \in \mathbb{F}^{k \times k}$ also has full rank.*
3. *For any $B \in \mathbb{F}_q^{n \times (n-k)}$ of full rank, the matrix $HB \in \mathbb{F}^{(n-k) \times (n-k)}$ also has full rank.*

**Proof.** For the first two claims, see [12, Lemma 2.10]. Lemma 7 says that $H$ is the generator matrix of a $[n, n-k]_\mathbb{F}$ MRD code $C^\perp$. The third claim follows by applying the second one to the dual code $C^\perp$. ◀

#### 2.2.0.2 Gabidulin codes.

The most famous MRD codes are Gabidulin codes, which are defined by using the evaluation of linearized polynomials. We briefly review the construction of Gabidulin codes [8] and extend it to a general field $\mathbb{F}/\mathbb{F}_q$.

▶ **Definition 13** (Gabidulin code over $\mathbb{F}$)**.** Let $0 < k \leq n$ be integers. Let $\mathbb{F}$ be an extension field of $\mathbb{F}_q$ such that $[\mathbb{F} : \mathbb{F}_q] \geq n$. Let $\alpha_1, \ldots, \alpha_n \in \mathbb{F}$ be linearly independent over $\mathbb{F}_q$. Define the $[n,k]_\mathbb{F}$ rank-metric code

$$\mathcal{G}_{n,k}(\alpha_1, \ldots, \alpha_n) := \left\{ \boldsymbol{x}_f = (f(\alpha_1), \ldots, f(\alpha_n)) : \ f \in \mathbb{F}[X] \text{ is } q\text{-linearized}, \deg_q(f) < k \right\},$$

---

[3] We remark that when $\mathbb{F} = \mathbb{F}_{q^m}$, there exists a Singleton bound, $|C| \leq q^{m(n-d+1)}$, that also applies to nonlinear rank-metric codes $C \subseteq \mathbb{F}^n$ [8]. However, this bound is given in terms of the size of the code, not the dimension, making it inapplicable when $\mathbb{F}$ is infinite.

where $f \in \mathbb{F}[X]$ is said to be $q$-linearized if it only contains monomials whose degrees are $q$-powers, and we define $\deg_q(f) = d$ if $\deg(f) = q^d$.

For a nonzero codeword $\boldsymbol{x}_f = (f(\alpha_1), \dots, f(\alpha_n)) \in \mathcal{G}_{n,k}(\alpha_1, \dots, \alpha_n)$, using the fact that $f$ is $q$-linearized, we have

$$\ker_{\mathbb{F}_q}(\boldsymbol{x}_f) = \left\{ (u_1, \dots, u_n) \in \mathbb{F}_q^n : f\left( \sum_{i=1}^n u_i \alpha_i \right) = 0 \right\}$$

whose dimension over $\mathbb{F}_q$ is bounded by $k-1$ since $\alpha_1, \dots, \alpha_n$ are linearly independent over $\mathbb{F}_q$ and $f$ has at most $\deg(f) \le q^{k-1}$ roots. So $\operatorname{rank}_{\mathbb{F}_q}(\boldsymbol{x}_f) \ge n-k+1$ by Lemma 6. This shows that Gabidulin codes are MRD codes.

The dual code of a Gabidulin code is also a Gabidulin code, which can be seen as an analogy of a Reed–Solomon code.

▶ **Theorem 14** (Duality of Gabidulin codes). *Let $\mathbb{F}$ be an extension field of $\mathbb{F}_q$, and let $\alpha_1, \dots, \alpha_n \in \mathbb{F}$ be linearly independent over $\mathbb{F}_q$. Then there exists $(\beta_1, \dots, \beta_n) \in \mathbb{F}^n \setminus \{0\}$ such that*

$$\sum_{i=1}^n \alpha_i^{q^{j-1}} \beta_i^{q^{h-1}} = 0 \qquad \text{for } (j,h) \in [k] \times [n-k]. \tag{2}$$

*The choice of $(\beta_1, \dots, \beta_n)$ satisfying (2) is unique up to a scalar in $\mathbb{F}_q \setminus \{0\}$. Moreover, $\beta_1, \dots, \beta_n$ are linearly independent over $\mathbb{F}_q$, and $\left(\beta_j^{q^{i-1}}\right)_{i \in [n-k], j \in [n]}$ is a parity-check matrix of $\mathcal{G}_{n,k}(\alpha_1, \dots, \alpha_n)$, i.e.,*

$$\mathcal{G}_{n,k}(\alpha_1, \dots, \alpha_n)^\perp = \mathcal{G}_{n,n-k}(\beta_1, \dots, \beta_n).$$

A proof can be found in [3, Lemma 2.7.2]. We present this proof for completeness.

**Proof of Theorem 14.** This holds for any extension field $\mathbb{F}$ no matter if $\mathbb{F}$ is finite or infinite. Let $\beta_1, \dots, \beta_n$ be the unique solution up to the scalar such that

$$\sum_{i=1}^n \alpha_i^{q^j} \beta_i = 0, \quad j = k+1-n, \dots, k-1. \tag{3}$$

The uniqueness is due to the fact that $(\alpha_i^{q^{k-j}})_{(i,j) \in [n] \times [n-1]}$ is a Moore matrix of rank $n-1$ if $\alpha_1, \dots, \alpha_n$ are $\mathbb{F}_q$-linearly independent. Then, for $j \in [k], h \in [n-k]$, we have

$$\sum_{i=1}^n \alpha_i^{q^j} \beta_i^{q^h} = \left( \sum_{i=1}^n \alpha_i^{q^{j-h}} \beta_j \right)^{q^h} = 0.$$

This is due to (3) and the fact that $k+1-n \le j-h \le k-1$. ◀

▶ **Definition 15** (Symbolic Gabidulin code). Let $0 < k \le n$. Let $\mathbb{F} = \mathbb{F}_q(X_1, \dots, X_n)$, where $X_1, \dots, X_n$ are transcendental and algebraically independent elements over $\mathbb{F}_q$. A $[n,k]_{\mathbb{F}}$ symbolic Gabidulin code is a $\mathbb{F}$-linear code with generator matrix $G = (X_j^{q^{i-1}})_{(i,j) \in [k] \times [n]}$, i.e.,

$$\mathcal{G}_{n,k}(X_1, \dots, X_n) := \left\{ \boldsymbol{x}_f = (f(X_1), \dots, f(X_n)) : \ f \in \mathbb{F}[X] \text{ is } q\text{-linearized}, \deg_q(f) < k \right\}.$$

## 2.3 Known Results on the List Decoding of Gabidulin Codes

For $G \in \mathbb{F}^{k\times n}$ over an extension field $\mathbb{F}/\mathbb{F}_q$, $A \in \mathbb{F}_q^{n\times d}$, and $V = \langle A\rangle \subseteq \mathbb{F}_q^n$, define $G_V \subseteq \mathbb{F}^n$ to be the column space of $GA$. The following results on the list decoding of symbolic Gabidulin codes can be found (implicitly) in [12].

▶ **Theorem 16** (Implicit in Theorem 1.16, [12])**.** *Let $\ell > 0$ be an integer. Let $\mathcal{G}_{n,k}(X_1, \dots, X_n)$ be a symbolic Gabidulin code with generator matrix $G$ and parity-check matrix $H$. Let $V_1, \dots, V_\ell$ be subspaces of $\mathbb{F}_q^n$, each of dimension at most $k$. Then,*

$$\dim_{\mathbb{F}}\left(\bigcap_{i\in[\ell]} G_{V_i}\right) = \max_{P_1\sqcup P_2\sqcup\cdots\sqcup P_s=[\ell]}\left(\sum_{i\in[s]}\dim_{\mathbb{F}_q}\left(\bigcap_{j\in P_i} V_j\right) - (s-1)k\right) \tag{4}$$

*where the maximum is taken over all possible partitions $P_1 \sqcup P_2 \sqcup \cdots \sqcup P_s$ of $[\ell]$. Let $V_1, \dots, V_\ell$ be subspaces of $\mathbb{F}_q^n$, each of dimension at most $n-k$. Then,*

$$\dim_{\mathbb{F}}\left(\bigcap_{i\in[\ell]} H_{V_i}\right) = \max_{P_1\sqcup P_2\sqcup\cdots\sqcup P_s=[\ell]}\left(\sum_{i\in[s]}\dim_{\mathbb{F}_q}\left(\bigcap_{j\in P_i} V_j\right) - (s-1)k\right). \tag{5}$$

▶ **Lemma 9** (Lemma 6.1, [12])**.** *Let $\mathbb{F}$ be an extension field of $\mathbb{F}_q$ and let $G \in \mathbb{F}^{k\times n}$. For $i = 1, \dots, \ell$, let $V_i$ be a subspace of $\mathbb{F}_q^n$ and let $A_i \in \mathbb{F}_q^{n\times \dim V_i}$ such that $V_i = \langle A_i\rangle$. Then, $G_{V_i} = \langle GA_i\rangle$ and*

$$\dim\left(\bigcap_{i\in[\ell]} G_{V_i}\right) = \sum_{i\in[\ell]}\dim G_{V_i} - \operatorname{rank}\left(G_{\{A_i\}_{i\in[\ell]}}\right), \tag{6}$$

*where we define the matrix* $G_{\{A_i\}_{i\in[\ell]}} := \begin{pmatrix} GA_1 & GA_2 & & & \\ GA_1 & & GA_3 & & \\ \vdots & & & \ddots & \\ GA_1 & & & & GA_\ell \end{pmatrix}.$

## 3 Characterization of the List Decodable Property

Let $\mathbb{F}$ be the extension field of $\mathbb{F}_q$. Let $C$ be a $[n,k]_{\mathbb{F}}$ code with generator matrix $G$ and parity-check matrix $H$. Assume $\boldsymbol{x}_iG \in \mathbb{F}^n, i = 1, \dots, \ell+1$ are $\ell+1$ codewords close to a vector $\boldsymbol{y} \in \mathbb{F}^n$, i.e.,

$$\sum_{i=1}^{\ell+1}\operatorname{rank}_{\mathbb{F}_q}(\boldsymbol{y} - \boldsymbol{x}_iG) \le \ell n(1-R+\varepsilon). \tag{7}$$

By replacing $\boldsymbol{y}$ with $\boldsymbol{y} - \boldsymbol{x}_1G$ and $\boldsymbol{x}_i$ with $\boldsymbol{x}_i - \boldsymbol{x}_1$ for $i > 1$, we may assume $\boldsymbol{x}_1 = 0$. Thus, (7) is equivalent to:

$$\operatorname{rank}(\boldsymbol{y}) + \sum_{i=2}^{\ell+1}\operatorname{rank}_{\mathbb{F}_q}(\boldsymbol{y} - \boldsymbol{x}_iG) \le \ell n(1-R+\varepsilon), \tag{8}$$

Let $V_i = \ker(\boldsymbol{y} - \boldsymbol{x}_iG) \subseteq \mathbb{F}_q^n$ be a vector space and $A_i \in \mathbb{F}_q^{n\times\dim(V_i)}$ such that $\langle A_i\rangle = V_i$. It follows that $\operatorname{rank}(A_i) = \dim(V_i) = n - \operatorname{rank}(\boldsymbol{y} - \boldsymbol{x}_iG)$ and $(\boldsymbol{y} - \boldsymbol{x}_iG)A_i = 0$. Since

$A_i^\top(\boldsymbol{y}^\top - G^\top \boldsymbol{x}_i^\top) = 0,$

$$\left(\begin{array}{c|c|c|c} A_1^\top & 0 & \cdots & 0 \\ A_2^\top & -A_2^\top G^\top & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ A_{\ell+1}^\top & 0 & \cdots & -A_{\ell+1}^\top G^\top \end{array}\right) \begin{pmatrix} \boldsymbol{y}^\top \\ \boldsymbol{x}_2^\top \\ \vdots \\ \boldsymbol{x}_{\ell+1}^\top \end{pmatrix} = 0. \tag{9}$$

Let the matrix above be denoted as $R_{G,\mathcal{V}_{[\ell+1]}}$ where $\mathcal{V}_{[\ell+1]} = (V_1, \ldots, V_{\ell+1})$. Since $A_i \in \mathbb{F}_q^{n\times \dim(V_i)}$, $R_{G,\mathcal{V}_{[\ell+1]}}$ is a $(\sum_{i=1}^{\ell+1}\dim(V_i)) \times (\ell k + n)$ matrix.

▶ **Lemma 10.** *Let $\rho \in (0,1)$, $\lambda \geq 0$, and $\ell$ be a positive integer. Let $C$ be an $[n,k]_{\mathbb{F}}$-linear code over a finite field $\mathbb{F}_q$ with generator matrix $G \in \mathbb{F}^{k\times n}$. Suppose $C$ is not $(\rho,\ell)$ average-radius list decodable in the rank metric and $\rho \leq \frac{\ell}{\ell+1}(1-(1+\lambda)\frac{k}{n})$. Then, there exist $t \in \{2,3,\ldots,\ell+1\}$ and $\mathbb{F}_q$-linear subspaces $V_1,\ldots,V_t \subseteq \mathbb{F}_q^n$ such that*

1. $\ker(R_{G,\mathcal{V}_{[t]}}) \neq 0$.
2. $\dim(\mathcal{V}_{[t]}) \geq (1+\lambda)(t-1)k$
3. $\dim(\mathcal{V}_J) \leq (1+\lambda)(|J|-1)k$ *for some non-empty set $J \subseteq [t]$.*

**Proof.** As $C$ is not $(\rho,\ell)$ average-radius list decodable in the rank metric, there exists a vector $\boldsymbol{y} \in \mathbb{F}^n$ and $\ell+1$ codewords $\boldsymbol{c}_1,\ldots,\boldsymbol{c}_{\ell+1} \in C$ such that $\sum_{i\in[\ell+1]} \mathrm{rank}_{\mathbb{F}_q}(\boldsymbol{y}-\boldsymbol{c}_i) \leq (\ell+1)\rho n$. Let $V_i = \ker(\boldsymbol{y}-\boldsymbol{c}_i)$ and we have $\sum_{i\in[\ell+1]}\dim(V_i) \geq (\ell+1)n(1-\rho)$. This implies that

$$\dim(\mathcal{V}_{[\ell+1]}) = \sum_{i\in[\ell+1]}\dim(V_i) - \dim(\sum_{i\in[\ell+1]} V_i) \geq \sum_{i\in[\ell+1]}\dim(V_i) - n \geq \ell(1+\lambda)k.$$

Thus, we can choose a minimal set $S \subseteq [\ell+1]$ of size at least 2 such that $\dim(V_S) \geq (1+\lambda)(|S|-1)k$. By permuting the codewords $\boldsymbol{c}_1,\ldots,\boldsymbol{c}_{\ell+1}$, we may assume that $S=[t]$. By the definition of $\dim(\mathcal{V}_J)$, $\dim(\mathcal{V}_J) = 0$ for any subset $J$ of size 1. Then, for any subset $J \subseteq [t]$, Item 3 holds due to the minimality of $S$. It remains to show that Item 1 holds. To see this, we first notice that $\boldsymbol{c}_i = \boldsymbol{x}_i G$ for some $\boldsymbol{x}_i \in \mathbb{F}_{q^m}^t$. Let $A_i \in \mathbb{F}_q^{n\times\dim(V_i)}$ such that $\langle A_i\rangle = V_i$. Since $V_i = \ker(\boldsymbol{y}-\boldsymbol{c}_i)$, we have $(\boldsymbol{y}-\boldsymbol{c}_i)A_i = (\boldsymbol{y}-\boldsymbol{x}_iG)A_i = 0$. Let $\boldsymbol{y}' = \boldsymbol{y}-\boldsymbol{x}_1G$ and $\boldsymbol{x}_i' = \boldsymbol{x}_i - \boldsymbol{x}_1$ for $i=2,\ldots,\ell+1$. Then $(\boldsymbol{y}',\boldsymbol{x}_2',\ldots,\boldsymbol{x}_t')^\top \in \ker(R_{G,\mathcal{V}_{[t]}})$. This completes the proof. ◀

▶ **Definition 17** (Reduced Matrix)**.** Let $\mathcal{V}_{[t]} = (V_1,\ldots,V_t)$, where each $V_i$ is a linear subspace of $\mathbb{F}_q^n$. Let $V \subseteq \mathbb{F}_q^n$ be a linear subspace and $\hat{V}_i = V_i \cap V$ be the intersection of $V_i$ and $V$. The reduced matrix $R_{G,\mathcal{V}_{[t]}}^V$ is defined as

$$R_{G,\mathcal{V}_{[t]}}^V = \left(\begin{array}{c|c|c|c} \hat{A}_1^\top & 0 & \cdots & 0 \\ \hat{A}_2^\top & -\hat{A}_2^\top G^\top & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ \hat{A}_t^\top & 0 & \cdots & -\hat{A}_t^\top G^\top \end{array}\right). \tag{10}$$

where $\hat{A}_i \in \mathbb{F}_q^{n\times\dim(\hat{V}_i)}$ of full rank with $\langle\hat{A}_i\rangle = \hat{V}_i$. If $V_J = \mathrm{span}_{\mathbb{F}_q}\{\boldsymbol{e}_i : i \in J\}$ for some $J \subseteq [n]$, we shorthand $R_{G,\mathcal{V}_{[t]}}^J := R_{G,\mathcal{V}_{[t]}}^{V_J}$ if no ambiguity occurs.

Let $A \subseteq \mathbb{F}_q^{n\times\dim(V)}$ with $\langle A\rangle = V$. Since the column vectors in $\hat{A}_i$ lie in $V = \langle A\rangle$, we may write $\hat{A}_i = AT_i$ where $T_i \in \mathbb{F}_q^{\dim(V)\times\dim(\hat{V}_i)}$ of full rank. Using the above notation, we have the following results.

▶ **Lemma 11.** *Let $G_1 = GA$ and $U_i = \langle T_i \rangle$ for $i = 1, \ldots, t$. Let $\mathcal{U}_{[t]} = (U_1, \ldots, U_t)$. Assume $\ker(R_{G_1,\mathcal{U}_{[t]}}) = 0$, i.e., there is no nonzero solution to*

$$\left(\begin{array}{c|c|c|c} T_1^\top & 0 & \cdots & 0 \\ T_2^\top & -T_2^\top G_1^\top & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ T_t^\top & 0 & \cdots & -T_t^\top G_1^\top \end{array}\right) \begin{pmatrix} \boldsymbol{y}^\top \\ \boldsymbol{x}_2^\top \\ \vdots \\ \boldsymbol{x}_t^\top \end{pmatrix} = 0. \tag{11}$$

*Then $\ker(R^V_{G,\mathcal{V}_{[t]}}) = 0$.*

**Proof.** Assume that there exists a solution $(\boldsymbol{y}, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_t) \in \ker(R^V_{G,\mathcal{V}_{[t]}})$. Let $\boldsymbol{y}' = \boldsymbol{y}A$. Then, $(\boldsymbol{y}', \boldsymbol{x}_2, \ldots, \boldsymbol{x}_t)^\top$ is a solution to (11) by observing

$$\hat{A}_i^\top G^\top = (AT_i)^\top G^\top = T_i^\top A^\top G^\top = T_i^\top (GA)^\top = T_i^\top G_1^\top. \qquad ◀$$

## 4 Connection to the Parity-Check Matrix

▶ **Definition 18.** Let $\mathbb{F}$ be the extension field of $\mathbb{F}_q$. Let $H$ be the parity-check matrix of a $[n,k]_{\mathbb{F}}$ code $C$. Let $\mathcal{V}_{[t]} = (V_1, \ldots, V_t)$ be a tuple of subspaces of $\mathbb{F}_q^n$. Assume that $D_i \in \mathbb{F}_q^{n \times \dim(V_i)}$ such that $\langle D_i \rangle = V_i$ for $i \in [t]$. Define the following matrix

$$M_{H,\mathcal{V}_{[t]}} = \left(\begin{array}{c|c|c|c|c} HD_1 & HD_2 & 0 & \cdots & 0 \\ HD_1 & 0 & HD_3 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ HD_1 & 0 & 0 & \cdots & HD_t \end{array}\right). \tag{12}$$

Since each $D_i$ is an $n \times \dim(V_i)$ matrix over $\mathbb{F}_q$, $M_{H,\mathcal{V}_{[t]}}$ is a $(t-1)(n-k) \times \sum_{i=1}^t \dim(V_i)$ matrix over $\mathbb{F}_q$.

The following theorem connects the matrices $M_{H,\mathcal{V}^\perp_{[t]}}$ and $R_{G,\mathcal{V}_{[t]}}$. See Appendix B for its proof.

▶ **Theorem 19.** *Let $\mathbb{F}$ be an extension field of $\mathbb{F}_q$. Let $G$ and $H$ be the generator and parity-check matrix of a $[n,k]_{\mathbb{F}}$ MRD code $C$, respectively. Let $\mathcal{V}_{[t]} = (V_1, \ldots, V_t)$ and $\mathcal{V}^\perp_{[t]} = (V_1^\perp, \ldots, V_t^\perp)$. Then, there is an injective $\mathbb{F}$-linear map $\phi : \ker(R_{G,\mathcal{V}_{[t]}}) \to \ker(M_{H,\mathcal{V}^\perp_{[t]}})$.*

We note that the matrix $R_{G,\mathcal{V}_{[t]}}$ is not a square matrix as $(t-1)k + n < \sum_{i \in [\ell+1]} \dim(V_i)$. This means that if $R_{G,\mathcal{V}_{[t]}}$ has full rank, there exists a reduced submatrix $R^V_{G,\mathcal{V}_{[t]}}$ of $R_{G,\mathcal{V}_{[t]}}$ that has the same rank as $R_{G,\mathcal{V}_{[t]}}$. The following theorem proves this claim provided that the dimension of $V$ is not too small. See Appendix C for its proof.

▶ **Theorem 20.** *Let $\mathbb{F} = \mathbb{F}_q(X_1, \ldots, X_n)$ where $X_1, \ldots, X_n$ are transcendental and algebraically independent elements over $\mathbb{F}_q$. Let $G = (X_j^{q^{i-1}})_{(i,j) \in [k] \times [n]}$ be the generator matrix of a $[n,k]_{\mathbb{F}}$ symbolic Gabidulin code. Let $\lambda > 0$ and $t > 1$. Assume that $\mathcal{V}_{[t]} = (V_1, \ldots, V_t)$ satisfies that $\dim(\mathcal{V}_{[t]}) \geq (1+\lambda)(t-1)k$ and $\dim(\mathcal{V}_J) \leq (|J|-1)(1+\lambda)k$ for all nonempty $J \subseteq [t]$. Let $V \subseteq \mathbb{F}_q^n$ be a linear space with $\dim(V) \geq n - \frac{\lambda k}{t-1}$. Then, $\ker(R^V_{G,\mathcal{V}_{[t]}}) = 0$.*

# 5 Random Assignment to Achieve the Capacity

## 5.1 Random Puncturing

Let $\{\boldsymbol{e}_1, \dots, \boldsymbol{e}_n\}$ be the standard basis of $\mathbb{F}_q^n$. Theorem 20 states that for any subspace $V \subseteq \mathbb{F}_q^n$ of dimension at least $n - \frac{\lambda k}{t-1}$, and $\mathcal{V}_{[t]} = (V_1, \dots, V_t)$ satisfying Item 2 and Item 3, we have $\ker(R^V_{G,\mathcal{V}_{[t]}}) = 0$. In this section, we focus on the subspace of the form $W_J := \mathrm{span}_{\mathbb{F}_q}\{\boldsymbol{e}_i : i \in J\}$ for some subset $J \subseteq [n]$. Recall that we shorthand $R^{W_J}_{G,\mathcal{V}}$ as $R^J_{G,\mathcal{V}}$. By focusing on the subset $J \subseteq [n]$, we are able to mimic the technique in [13] to bound the probability that $R^J_{G,\mathcal{V}_{[t]}}$ is not of full rank when selecting the value of $X_i$ uniformly at random. The connection between $R^J_{G,\mathcal{V}_{[t]}}$ and $R_{G,\mathcal{V}_{[t]}}$ can be found in the following lemma.

▶ **Lemma 12.** *Let $\mathcal{V}_{[t]} = (V_1, \dots, V_t) \in (\mathbb{F}_q^n)^t$ and $V \subseteq \mathbb{F}_q^n$. Then, there exist $A_i$ and $\hat{A}_i$ in* (9) *and* (10) *such that $R^V_{G,\mathcal{V}_{[t]}}$ is a submatrix of $R_{G,\mathcal{V}_{[t]}}$.*

**Proof.** From Lemma 4, we can find $A_i \in \mathbb{F}_q^{n\times \dim(V_i)}$ and its submatrix $\hat{A}_i \in \mathbb{F}_q^{n\times\dim(\hat{V}_i)}$ such that $\langle A_i\rangle = V_i$, $\langle \hat{A}_i\rangle = \hat{V}_i$. This implies that $(\hat{A}_i^\top, 0, \dots, 0, -\hat{A}_i^\top G^\top, 0, \dots, 0)$ is a submatrix of $(A_i^\top, 0, \dots, 0, -A_i^\top G^\top, 0, \dots, 0)$. In view of the expression of $R^V_{G,\mathcal{V}_{[t]}}$ and $R_{G,\mathcal{V}_{[t]}}$, we conclude that $R^V_{G,\mathcal{V}_{[t]}}$ is a submatrix of $R_{G,\mathcal{V}_{[t]}}$. ◀

Next, we define the faulty index which was first proposed in [13].

▶ **Definition 21** (Faulty index)**.** Assume $r \ge \ell$. Let $A \in \mathbb{F}_q(X_1, \dots, X_n)^{r\times\ell}$ be a matrix such that $\mathrm{rank}(A) = \ell$ and the entries of $A$ are in $\mathbb{F}_q[X_1, \dots, X_n]$. For $\alpha_1, \dots, \alpha_n \in \mathbb{F}_{q^m}$, we say $i \in [n]$ is the faulty index of $A$ (with respect to $\alpha_1, \dots, \alpha_n$) if $A|_{X_1=\alpha_1,\dots,X_{i-1}=\alpha_{i-1}}$ has full (column) rank but $A|_{X_1=\alpha_1,\dots,X_i=\alpha_i}$ does not.

**Algorithm 1** Output faulty indices

---

**Input**: $\mathcal{V} = (V_1, \dots, V_t) \subseteq (\mathbb{F}_q^n)^t$, $\alpha_1, \dots, \alpha_n \in \mathbb{F}_{q^m}$, and positive integer $r$
**Output**: "Success" or $(i_1, \dots, i_r) \in [n]^r$
Let $G = (X_j^{q^{i-1}})_{(i,j)\in[k]\times[n]}$ and $J = [n]$.
**for** $j = 1$ to $r$, **do**
  **if** $\mathrm{rank}(R^J_{G,\mathcal{V}}) < (t-1)k + n$ **then**
    Output "Fail" and halt.
  **else if** $i \in [n]$ is the faulty index of $R^J_{G,\mathcal{V}}$ **then**
    $i_j = i$ and $J = J \setminus \{i\}$.
  **else**
    Output "Success" and halt.
  **end if**
**end for**
Output $(i_1, \dots, i_r)$.

---

▶ **Lemma 13.** *Let $\lambda \ge 0$ and let $t \ge 1$ be an integer. Let $\mathcal{V}_{[t]} = (V_1, \dots, V_t) \subseteq (\mathbb{F}_q^n)^t$ such that $\dim(\mathcal{V}_{[t]}) \ge (1+\lambda)(t-1)k$ and $\dim(\mathcal{V}_J) \le (1+\lambda)(|J|-1)k$ for all nonempty $J \subseteq [t]$. Let $r$ be a positive integer with $r \le \frac{\lambda k}{t-1} + 1$. Then, for all $\alpha_1, \dots, \alpha_n \in \mathbb{F}_{q^m}$, running Algorithm 1 on the input $\mathcal{V}_{[t]}$, $\alpha_1, \dots, \alpha_n$, and $r$ yields the following two possible scenarios:*

1. *Algorithm 1 outputs "Success". In this case, $R_{G,\mathcal{V}_{[t]}}|_{X_1=\alpha_1,\dots,X_n=\alpha_n}$ has full rank.*

2. *Algorithm 1 outputs an $r$-tuple $(i_1,\dots,i_r)\in\binom{[n]}{r}$. In this case, for each $j\in[r]$, $i_j$ is the faulty index of $R^{S_j}_{G,\mathcal{V}_{[t]}}$ for $S_j=[n]\setminus\{i_1,\dots,i_{j-1}\}$.*

**Proof.** Assume the algorithm reaches the $j$-th round of the loop. At the beginning, we have $|J|\ge n-j+1\ge n-r+1\ge n-\frac{\lambda k}{t-1}$. Then by Lemma 11 and the fact that $G$ is the generator matrix of a symbolic Gabidulin code, $R^J_{G,\mathcal{V}}$ has full rank and thus the algorithm never outputs "Fail". Suppose that the algorithm outputs "Success" and halts in the $j$-th round. This means that the faulty index of $R^J_{G,\mathcal{V}}$ does not exist in this round. This implies that $R_{G,\mathcal{V}}|_{X_1=\alpha_1,\dots,X_n=\alpha_n}$ has full rank. It remains to consider the case where the algorithm outputs a $r$-tuple $(i_1,\dots,i_r)$. For $j\in[r]$, the index $i_j$ is chosen to be the faulty index of $R^{S_j}_{G,\mathcal{V}}$, where $S_j=[n]\setminus\{i_1,\dots,i_{j-1}\}$. The distinctness of $i_1,\dots,i_r$ is due to the fact that if $i\notin S_j$, then $R^{S_j}_{G,\mathcal{V}}$ does not contain $X_i$. ◀

▶ **Lemma 14.** *Suppose $m\ge n$ and $(\alpha_1,\dots,\alpha_n)$ are chosen uniformly at random in $\mathbb{F}_{q^m}$. Then, for any $r$-tuple $(i_1,\dots,i_r)\in\binom{[n]}{r}$ and $(V_1,\dots,V_t)\in(\mathbb{F}_q^n)^t$, the probability that Algorithm 1 outputs $(i_1,\dots,i_r)$ given the input $(V_1,\dots,V_t)$, $\alpha_1,\dots,\alpha_n$ and $r$ is at most $\left(\frac{(t-1)kq^{k-1}}{q^m}\right)^r$.*

**Proof.** For $j\in[r]$, define the following:
1. $S_j:=[n]\setminus\{i_1,\dots,i_{j-1}\}$.
2. Let $M_j$ be the smallest nonsingular maximal minor of $R^{S_j}_{G,\mathcal{V}}$ in the lexicographic order. The same argument in Lemma 13 implies that for $j\in[r]$, $R^{S_j}_{G,\mathcal{V}}$ has full rank and hence $M_j$ exists.
3. Let $E_j$ be the event that $\det(M_j|_{X_1=\alpha_1,\dots,X_{i_j-1}=\alpha_{i_j-1}})\ne$ but $\det(M_j|_{X_1=\alpha_1,\dots,X_{i_j}=\alpha_{i_j}})$ is zero.

Note that if $(i_1,\dots,i_r)$ is output by the algorithm, then $E_1,\dots,E_r$ occurs. So it suffices to prove that $\Pr[E_1\wedge\cdots\wedge E_r]\le\left(\frac{(t-1)kq^{k-1}}{q^m}\right)^r$.

Let $(j_1,j_2,\dots,j_r)$ be a permutation of $(1,2,\dots,r)$ such that $i_{j_1}<\cdots<i_{j_r}$, i.e., $i_{j_\ell}$ is the $\ell$-th smallest index among $i_1,\dots,i_r$ for $\ell\in[r]$. For $\ell\in\{0,1,\dots,r\}$, define $F_\ell:=E_{j_1}\wedge\cdots\wedge E_{j_\ell}$, where we let $F_0$ be the event that always occurs. Then $F_r=E_{j_1}\wedge\cdots\wedge E_{j_r}=E_1\wedge\cdots\wedge E_r$. If $\Pr[F_r]=0$ then we are done. So assume $\Pr[F_r]>0$. By definition, if $F_\ell$ occurs and $\ell'<\ell$, then $F_{\ell'}$ also occurs. So $\Pr[F_\ell]>0$ for all $\ell\in\{0,1,\dots,r\}$. Note

$$\Pr[E_1\wedge\cdots\wedge E_r]=\Pr[F_r]=\prod_{\ell=1}^{r}\frac{\Pr[F_\ell]}{\Pr[F_{\ell-1}]}.$$

So it suffices to prove that $\frac{\Pr[F_\ell]}{\Pr[F_{\ell-1}]}\le\frac{(t-1)kq^{k-1}}{q^m}$ for $\ell\in[r]$.

Fix $\ell\in[r]$ and let $j=j_\ell$. Let $T$ be the set of all $\beta=(\beta_1,\dots,\beta_{i_j-1})\in\mathbb{F}_q^{i_j-1}$ such that $\Pr\left[(\alpha_{<i_j}=\beta)\wedge F_{\ell-1}\right]>0$, where $\alpha_{<i_j}=\beta$ is a shorthand for $(\alpha_1=\beta_1)\wedge\cdots\wedge(\alpha_{i_j-1}=\beta_{i_j-1})$. Note that for $\beta\in T$, the event $(\alpha_{<i_j}=\beta)\wedge F_{\ell-1}$ is simply $\alpha_{<i_j}=\beta$ since $F_{\ell-1}=E_{j_1}\wedge\cdots\wedge E_{j_{\ell-1}}$ depends only on $\alpha_1,\dots,\alpha_{i_{j_{\ell-1}}}$ and is bound to happen conditioned on $\alpha_{<i_j}=\beta$. We then have

$$\begin{aligned}\frac{\Pr[F_\ell]}{\Pr[F_{\ell-1}]}&=\frac{\sum_{\beta\in S}\Pr\left[(\alpha_{<i_j}=\beta)\wedge F_\ell\right]}{\sum_{\beta\in S}\Pr\left[(\alpha_{<i_j}=\beta)\wedge F_{\ell-1}\right]}=\frac{\sum_{\beta\in S}\Pr\left[(\alpha_{<i_j}=\beta)\wedge E_j\right]}{\sum_{\beta\in S}\Pr\left[\alpha_{<i_j}=\beta\right]}\\&\le\max_{\beta\in S}\frac{\Pr\left[(\alpha_{<i_j}=\beta)\wedge E_j\right]}{\Pr\left[\alpha_{<i_j}=\beta\right]}=\max_{\beta\in S}\Pr\left[E_j\mid\alpha_{<i_j}=\beta\right].\end{aligned}$$

Fix $\beta = (\beta_1, \ldots, \beta_{i_j-1}) \in T$. We just need to prove that $\Pr\left[E_j \mid \alpha_{<i_j} = \beta\right] \le \frac{(t-1)kq^{k-1}}{q^m}$. Let

$$Q := \det(M_j|_{X_1=\beta_1,\ldots,X_{i_j-1}=\beta_{i_j-1}}) \in \mathbb{F}_q[X_{i_j}, \ldots, X_n].$$

If $Q = 0$, then $E_j$ never occurs conditioned on $\alpha_{<i_j} = \beta$ and we are done. So assume $Q \neq 0$. View $Q$ as a polynomial in $X_{i_j+1}, \ldots, X_n$ over the ring $\mathbb{F}_q[X_{i_j}]$, and let $Q_0 \in \mathbb{F}_q[X_{i_j}]$ be the coefficient of a nonzero term of $Q$. Then conditioned on $\alpha_{<i_j} = \beta$, the event $E_j$ occurs only if $\alpha_{i_j}$ is a root of $Q_0 \neq 0$. Note that $\deg Q_0 \le \deg_{X_{i_j}} Q \le \deg_{X_{i_j}}(\det(M_j))$, which is bounded by $(t-1)kq^{k-1}$ from the expression of $R^{S_j}_{G,\mathcal{V}}$. Also note that conditioned on $\alpha_{<i_j} = \beta$, the random variable $\alpha_{i_j}$ is uniformly distributed over $\mathbb{F}_q^m$. It follows that $\Pr\left[E_j \mid \alpha_{<i_j} = \beta\right] \le \frac{(t-1)kq^{k-1}}{q^m}$. ◀

▶ **Corollary 22.** *Under the notations and conditions in Lemma 14, suppose $m \ge n$ and $(\alpha_1, \ldots, \alpha_n)$ is chosen uniformly at random, then*

$$\Pr[\ker(R_{G,\mathcal{V}}|_{X_1=\alpha_1,\ldots,X_n=\alpha_n}) \neq 0] \le \left((t-1)knq^{k-m}\right)^r.$$

**Proof.** Take a union bound over sequences $(i_1, \ldots, i_r) \in \binom{[n]}{r}$, by Lemma 14, the probability that Algorithm 1 outputs a faulty sequence on the input $V_1, \ldots, V_t$ and $\alpha_1, \ldots, \alpha_n$ is at most $n^r \times ((t-1)kq^{k-m})^r$. If this doesn't happen, by Lemma 13, $\ker(R_{G,\mathcal{V}}|_{X_1=\alpha_1,\ldots,X_n=\alpha_n}) \neq 0$. ◀

## 5.2 Application to List Decoding

We are ready to prove our main results.

▶ **Theorem 23.** *Let $\varepsilon \in (0,1), c > 1$ and $n, k, m, \ell$ be positive integers with $k \le n$ and $m \ge \frac{c\ell(\ell+1)n}{\varepsilon}$. Then with probability at least $1 - q^{-\Omega(n)}$, a randomly punctured Gabidulin code $C \subseteq \mathbb{F}_{q^m}^n$ with rate $R := \frac{k}{n}$ is $(\frac{\ell}{\ell+1}(1 - R - \varepsilon), \ell)$ average-radius list decodable.*

**Proof.** Let $\lambda = \frac{\varepsilon}{R} = \frac{\varepsilon k}{n}$. By Lemma 10, if $C$ with generator matrix $G$ is not $(\frac{\ell}{\ell+1}(1-R-\varepsilon), \ell)$ average-radius list decodable in the rank metric, then, there exist $t \in \{2, 3, \ldots, \ell+1\}$ and $\mathbb{F}_q$-linear subspaces $V_1, \ldots, V_t \subseteq \mathbb{F}_q^n$ such that

1. $\ker(R_{G,\mathcal{V}_{[t]}}) \neq 0$.
2. $\dim(\mathcal{V}_{[t]}) \ge (1 + \lambda)(t-1)k$
3. $\dim(\mathcal{V}_J) \le (1 + \lambda)(|J| - 1)k$ for some non-empty set $J \subseteq [t]$.

Choose $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_{q^m}$ uniformly at random. The probability that $\alpha_1, \ldots, \alpha_n$ are $\mathbb{F}_q$-linearly dependent is at most $nq^{(n-m)} = q^{-\Omega(n)}$. Let $\bar{G} = (\alpha_j^{q^{i-1}})_{(i,j)\in[k]\times[n]}$. To prove this theorem,it suffices to show that Items 1–3 simultaneously hold with probability at most $q^{-O(n^2)}$. We fix $t \in \{2, 3, \ldots, \ell+1\}$ and $V_1, \ldots, V_t \subseteq \mathbb{F}_q^n$ satisfying Item 2 and Item 3. Let $r = \lfloor \frac{\lambda k}{t-1} + 1 \rfloor \ge \frac{\lambda k}{t-1} = \frac{\varepsilon n}{t-1}$. Observe that $R_{\bar{G},\mathcal{V}_{[t]}} = R_{G,\mathcal{V}_{[t]}}|_{X_1=\alpha_1,\ldots,X_n=\alpha_n}$ where $G = (X_j^{q^{i-1}})_{(i,j)\in[k]\times[n]}$. By Corollary 22, the probability that $\ker(R_{\bar{G},\mathcal{V}_{[t]}}) \neq 0$ holds is at most $(\ell knq^{k-m})^r \le (\ell knq^{k-m})^{\frac{\varepsilon n}{\ell}}$, where we use the fact that $r \ge \frac{\varepsilon n}{\ell}$. The number of $t$-tuples $\mathcal{V}_{[t]}$, where $t$ ranges over $\{2, \ldots, \ell+1\}$, is bounded by $\sum_{t=2}^{\ell+1}(q^{n^2})^t \le 2q^{(\ell+1)n^2}$. By the union bound, the probability that Items 1–3 hold for some $t \in \{2, \ldots, \ell+1\}$ and $V_1, \ldots, V_t \subseteq \mathbb{F}_q^n$ is at most $2q^{(\ell+1)n^2} \times (\ell knq^{k-m})^{\frac{\varepsilon n}{\ell}} + nq^{n-m} = 2(knq^{k+n\ell(\ell+1)/\varepsilon - m})^{\varepsilon n/\ell} + q^{-\Omega(n)} = q^{-\Omega(n)}$ as $m \ge \frac{cn\ell(\ell+1)}{\varepsilon}$ for some $c > 1$. ◀

# A Field Size Lower Bound for Capacity-Achieving Rank-Metric Codes

We prove a lower bound on the field size of capacity achieving rank-metric codes by adapting the argument in [1]. We first prove a lower bound for rank-metric codes with large distance in Theorem 24. Then, we remove this distance requirement in Corollary 25.

▶ **Theorem 24.** *Let $\ell \geq 2$. For any $r \in [0,1]$, any rank-metric code $C \subseteq \mathbb{F}_{q^m}^n$ of rate $R$ and minimum distance at least $(1-R-\varepsilon)n+1$ that is $\left(\frac{\ell(1-R-\varepsilon)}{\ell+1}, \ell\right)$-avearge-radius list decodable must have $m = \Omega(\frac{Rn}{\varepsilon})$.*

**Proof.** Fix a subspace $V_0 \subseteq \mathbb{F}_q^n$ of dimension $b := 4\varepsilon n$. Choose a subspace $\overline{V}_0$ such that $V_0 \oplus \overline{V}_0 = \mathbb{F}_q^n$. Let $\alpha = R - \varepsilon$ and $\beta = R + \varepsilon$. Let $\mathcal{F}$ be the collection of subspaces $V \subseteq \overline{V}_0$ of dimension $\alpha n$ such that for any pair of vector spaces $V_1, V_2 \in \mathcal{F}_1$, $\dim(V_1 + V_2) \geq \beta n$. By Corollary 8, the size of $\mathcal{F}$ can be at least $q^{\Omega((\alpha-\alpha^2-4\varepsilon-o(1))n^2)}$. It suffices to prove that $\ell q^{bm} \geq |\mathcal{F}|/2$, as this would imply $m = \Omega(\frac{Rn}{\varepsilon})$.

Assume to the contrary that $\ell q^{bm} < |\mathcal{F}|/2$. Let $M$ be uniformly distributed from $C$. For a fixed subspace $V \in \mathcal{F}$, let $A \in \mathbb{F}_q^{n\times \alpha n}$ such that $\langle A \rangle = V$. Let $E_V$ be the event that there exists a codeword $M_1 \in C$ different from $M$ such that $MA = M_1 A$, i.e., $(M - M_1)A = 0$. If $E_V$ does not hold, then $M$ is uniquely determined by $MA \in \mathbb{F}_q^{m\times \alpha n}$. As the number of possible values of $MA$ is at most $q^{\alpha nm}$ and $|C| = q^{Rmn}$, we have

$$\Pr[\neg E_V] \leq \frac{q^{\alpha mn}}{q^{Rmn}} = q^{-\varepsilon Rmn}.$$

Therefore, over random $M \in C$, the expected number of $V \in \mathcal{F}$ such that $E_V$ happens is $\sum_{V\in\mathcal{F}}(1 - \Pr[\neg E_V]) \geq |\mathcal{F}|/2$. Then, we can fix a codeword $M \in C$ such that the size of the set

$$\mathcal{F}_M := \{V \in \mathcal{F} : E_V \text{ happens}\}$$

is at least $|\mathcal{F}|/2$.

Let $A_0 \in \mathbb{F}_q^{n\times b}$ such that $\langle A_0 \rangle = V_0$. By the definition of $\mathcal{F}_M$, for each $V \in \mathcal{F}_M$, there exists a codeword $M_V \neq M$ such that the kernel subspace of $M - M_V$ contains $V$. Since $M_V A_0 \in \mathbb{F}_q^{m\times b}$ for any codeword $M_V$ and $\ell q^{bm} < |\mathcal{F}|/2 \leq |\mathcal{F}_M|$, by the pigeonhole principle, there exists distinct $V_1, \dots, V_\ell \in \mathcal{F}_M$ such that $M_{V_1} A_0 = \dots = M_{V_\ell} A_0$. Moreover, by the definition of $\mathcal{F}_M$, for $i = 1, \dots, \ell$, there exists $A_i \in \mathbb{F}_q^{n\times \alpha n}$ with $\langle A_i \rangle = V_i$ such that $(M - M_{V_i})A_i = 0$.

Assume $M_{V_i} = M_{V_j}$ for some $i \neq j$. Then $(M - M_{V_i})A_i = 0$ and $(M - M_{V_i})A_j = 0$. Let $A \in \mathbb{F}_q^{n\times \dim(V_i+V_j)}$ such that $\langle A \rangle = V_i + V_j$. As the columns of $A$ are in $V_i + V_j = \langle A_i \rangle + \langle A_j \rangle$, we have $(M - M_{V_i})A = 0$, i.e., $V_i + V_j$ is contained in the kernel subspace of $M - M_{V_i}$. Since $M$ and $M_{V_i}$ are in code $C$ of minimum distance at least $(1-R-\varepsilon)n+1$, we have $\operatorname{rank}(M - M_{V_i}) \geq (1-R-\varepsilon)n+1$. This implies that the kernel subspace of $M - M_{V_i}$ is at most $(R+\varepsilon)n - 1$. So $\dim(V_i + V_j) \leq (R+\varepsilon)n - 1$. However, as $V_i, V_j \in \mathcal{F}$ and thus $\dim(V_i + V_j) \geq \beta n = (R+\varepsilon)n$, which yields a contradiction. Thus, we conclude that $M_{V_1}, \dots, M_{V_\ell}$ are all distinct.

Since $\overline{V}_0 \cap V_0 = \{0\}$, there exists $B_0 \in \mathbb{F}_q^{n\times(n-b)}$ such that $\langle B_0 \rangle = \overline{V}_0$ and $\begin{pmatrix} A_0 & B_0 \end{pmatrix} \in \mathbb{F}_q^{n\times n}$ has full rank. Let $Y \in \mathbb{F}_q^{m\times n}$ such that $(M_{V_1} - Y)A_0 = \dots = (M_{V_\ell} - Y)A_0 = 0$ and $(M - Y)B_0 = 0$. This can be achieved by choosing $Y = \begin{pmatrix} M_{V_1}A_0 & MB_0 \end{pmatrix} \begin{pmatrix} A_0 & B_0 \end{pmatrix}^{-1}$.

For $i \in [\ell]$, we have $(M - Y)A_i = 0$ since $\langle A_i \rangle = V_i$, $V_i \subseteq \overline{V}_0$, $\overline{V}_0 = \langle B_0 \rangle$, and $(M - Y)B_0 = 0$. And for $i \in [\ell]$, we know $(M - M_{V_i})A_i = 0$, which implies

$$(M_{V_i} - Y)A_i = (M_{V_i} - M)A_i + (M - Y)A_i = 0 \quad \text{and} \quad (M_{V_i} - Y)A_0 = 0.$$

Since $V_0 \cap \langle V_i \rangle \subseteq V_0 \cap \overline{V}_0 = \{0\}$ for $i \in [\ell]$, we have $\dim(V_0 + V_i) = \dim V_0 + \dim V_i = b + \alpha n$ and hence

$$\operatorname{rank}(M_{V_i} - Y) \le n - (b + \alpha n) \le (1 - R - 3\varepsilon)n,$$

as $b = 4\varepsilon n$. As $(M - Y)B_0 = 0$, we have $\operatorname{rank}(M - Y) \le n - \dim(\overline{V}_0) = b = 4\varepsilon n$. It follows that

$$\operatorname{rank}(M - Y) + \sum_{i=1}^{\ell} \operatorname{rank}(M_{V_i} - Y) \le 4\varepsilon n + \ell(1 - R - 3\varepsilon) \le \ell(1 - R - \varepsilon)n.$$

as $\ell \ge 2$. This contradicts the claim that $C$ is $\left(\frac{\ell(1-R-\varepsilon)}{\ell+1}, \ell\right)$-avearge-radius list decodable. ◀

We now show how to remove the minimum distance requirement in Theorem 24.

▶ **Corollary 25.** *Let $\ell \ge 2$. For any $r \in [0, 1]$, any rank-metric code $C \subseteq \mathbb{F}_{q^m}^n$ of rate $R$ that is $\left(\frac{\ell(1-R-\varepsilon)}{\ell+1}, \ell\right)$-avearge-radius list decodable must have $m = \Omega(\frac{Rn}{\varepsilon})$.*

**Proof.** Compared to Theorem 24, this statement only remove the minimum distance requirement. Thus, if we find a subcode of $C$ with minimum distance $(1 - R - \varepsilon)$ and the same rate $R$, then we can apply the argument in Theorem 24 directly to obtain the desired result. To achieve this goal, we prove the claim that for any $M \in C$, there are at most $\ell - 1$ codewords $T_1, \ldots, T_{\ell-1}$ in $C$ that is within minimum distance at most $(1 - R - \varepsilon)n$ from $M_1$. Assume not and we find $T_1, \ldots, T_\ell$ such that $\operatorname{rank}(M - T_i) \le (1 - R - \varepsilon)n$. Let $M$ be the center and we claim that

$$\operatorname{rank}(M - M) + \sum_{i=1}^{\ell} \operatorname{rank}(M - T_i) \le \ell(1 - R - \varepsilon).$$

Thus, $C$ is not $\left(\frac{\ell(1-R-\varepsilon)}{\ell+1}, \ell\right)$-avearge-radius list decodable code and a contradiction happens. Therefore, we can find a subcode $C_1 \subseteq C$ of size at least $\frac{|C|}{\ell}$ such that the minimum distance of $C_1$ is at least $(1 - R - \varepsilon)n$. We can apply the same argument in Theorem 24 to obtain the desired result. ◀

## B Proof of Theorem 19

**Proof.** For $i \in [t]$, let $A_i \subseteq \mathbb{F}_q^{n \times \dim V_i}$ such that $\langle A_i \rangle = V_i$. By Lemma 2, there exist full-rank matrices $B_i \in \mathbb{F}_q^{n \times \dim(V_i^\perp)}$, $C_i \in \mathbb{F}_q^{n \times \dim(V_i)}$, and $D_i \in \mathbb{F}_q^{n \times \dim(V_i^\perp)}$ such that $C_i A_i^\top + D_i B_i^\top = I_n$ and $\langle D_i \rangle = V_i^\perp$. Define the linear map $\phi$ such that it sends a row vector $\boldsymbol{v} := (\boldsymbol{y}, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_t) \in \ker(R_{G, \mathcal{V}_{[t]}})$ to

$$\phi(\boldsymbol{y}, \boldsymbol{x}_2, \cdots, \boldsymbol{x}_t) = \Big( -\boldsymbol{y}B_1, (\boldsymbol{y} - \boldsymbol{x}_2 G)B_2, \ldots, (\boldsymbol{y} - \boldsymbol{x}_t G)B_t \Big).$$

Since $B_i$ is an $n \times (n - \dim(V_i))$ matrix over $\mathbb{F}_q$, $\phi(\boldsymbol{v})$ is a vector of length $\sum_{i=1}^t (n - \dim(V_i))$ which is exactly the number of columns of $M_{H, \mathcal{V}_{[t]}^\perp}$. Next, we show that $\phi(\boldsymbol{v})$ belongs to $\ker(M_{H, \mathcal{V}_{[t]}^\perp})$. To see this, we observe that $H\boldsymbol{y}^\top = H(\boldsymbol{y} - \boldsymbol{x}_2 G)^\top = \cdots = H(\boldsymbol{y} - \boldsymbol{x}_t G)^\top$. Also,

$$H\boldsymbol{y}^\top = H \begin{pmatrix} C_1 & D_1 \end{pmatrix} \begin{pmatrix} A_1^\top \\ B_1^\top \end{pmatrix} \boldsymbol{y}^\top = H \begin{pmatrix} C_1 & D_1 \end{pmatrix} \begin{pmatrix} 0 \\ B_1^\top \boldsymbol{y}^\top \end{pmatrix} = H D_1 B_1^\top \boldsymbol{y}^\top$$

and

$$H(\boldsymbol{y}-\boldsymbol{x}_iG)^\top = H\begin{pmatrix}C_i & D_i\end{pmatrix}\begin{pmatrix}A_i^\top\\ B_i^\top\end{pmatrix}(\boldsymbol{y}-\boldsymbol{x}_iG)^\top = H\begin{pmatrix}C_i & D_i\end{pmatrix}\begin{pmatrix}0\\ B_i^\top(\boldsymbol{y}-\boldsymbol{x}_iG)^\top\end{pmatrix}$$
$$= HD_iB_i^\top(\boldsymbol{y}-\boldsymbol{x}_iG)^\top.$$

This implies that $HD_1B_1^\top\boldsymbol{y}^\top = HD_iB_i^\top(\boldsymbol{y}-\boldsymbol{x}_iG)^\top$ for $i=2,\dots,t$, and thus $\phi(\boldsymbol{v})$ belongs to $\ker(M_{H,\mathcal{V}_{[t]}^\perp})$.

It remains to show that $\phi$ is an injection. It suffices to show that $\phi(\boldsymbol{v})=0$ implies $\boldsymbol{v}=0$ as $\phi$ is a linear map. As $y^\top = \begin{pmatrix}C_1 & D_1\end{pmatrix}\begin{pmatrix}A_1^\top\\ B_1^\top\end{pmatrix}\boldsymbol{y}^\top = \begin{pmatrix}C_1 & D_1\end{pmatrix}\begin{pmatrix}0\\ B_1^\top\boldsymbol{y}^\top\end{pmatrix}$, we know that $\boldsymbol{y}B_1=0$ implies $\boldsymbol{y}=0$. Similarly, as $(\boldsymbol{y}-\boldsymbol{x}_iG)^\top = \begin{pmatrix}C_i & D_i\end{pmatrix}\begin{pmatrix}A_i^\top\\ B_i^\top\end{pmatrix}(\boldsymbol{y}-\boldsymbol{x}_iG)^\top = \begin{pmatrix}C_i & D_i\end{pmatrix}\begin{pmatrix}0\\ B_i^\top(\boldsymbol{y}-\boldsymbol{x}_iG)^\top\end{pmatrix}$, we know that $(\boldsymbol{y}-\boldsymbol{x}_iG)B_i=0$ implies $\boldsymbol{y}-\boldsymbol{x}_iG=0$ for $i=2,\dots,t$. So $\phi(\boldsymbol{v})=0$ implies $\boldsymbol{v}=0$. ◀

## C Proof of Theorem 20

**Proof.** Let $n'=\dim(V)$. Let $A\subseteq\mathbb{F}_q^{n\times n'}$ such that $\langle A\rangle = V$. Let $\mathcal{U}_{[t]}=(U_1,\dots,U_t)\subseteq(\mathbb{F}_q^{n'})^t$ be given in Lemma 11 and we have $\dim(U_i)=\dim(V_i\cap V)$. Note that

$$\dim(\mathcal{U}_{[t]}) = \sum_{i\in[t]}\dim(U_i) - \dim(\sum_{i=1}^t U_i) \ge \dim(\mathcal{V}_{[t]}) - (n-\dim(V))(t-1) \ge (1+\lambda)(t-1)k - \lambda k \tag{13}$$

and

$$\dim(\mathcal{U}_J)\le\dim(\mathcal{V}_J)\le(1+\lambda)(|J|-1)k \tag{14}$$

for any nonempty set $J\subseteq[t]$.

By Lemma 11, to prove $\ker(R^V_{G,\mathcal{V}_{[t]}})=0$, it suffices to show that $\ker(R_{G_1,\mathcal{U}_{[t]}})=0$ for $G_1=GA$. Here $GA=(Z_j^{q^{i-1}})_{[k]\times[n']}$ is also a generator matrix of a symbolic Gabidulin code $C$ by letting $(Z_1,\dots,Z_{n'})=(X_1,\dots,X_n)A$. Moreover, by replacing $\mathbb{F}_q^{n'}$ with $V' := \sum_{i=1}^t U_i$ and identifying view $U_i$ as a subspace of $V'$, we may assume $\sum_{i=1}^t U_i = \mathbb{F}_q^{n'}$.

It follows from (13) and (14) that $\dim(U_i)\ge\dim(\mathcal{U}_{[t]})-\dim(\mathcal{U}_{[t]/\{i\}})\ge k$. So $\dim(U_i^\perp)\le n'-k$. Let $H_1$ be the parity-check matrix of $C$, i.e., $G_1H_1^\top=0$. Define $\mathcal{U}_{[t]}^\perp=(U_1^\perp,\dots,U_t^\perp)$. Then, by Definition 18, we have

$$M_{H_1,\mathcal{U}_{[t]}^\perp} = \left(\begin{array}{c|c|c|c|c} H_1D_1 & H_1D_2 & 0 & \cdots & 0\\ H_1D_1 & 0 & H_1D_3 & \cdots & 0\\ \vdots & \vdots & \vdots & \ddots & \vdots\\ H_1D_1 & 0 & 0 & \cdots & H_1D_t \end{array}\right) \tag{15}$$

where $D_i\subseteq\mathbb{F}_q^{n'\times\dim(U_i^\perp)}$ with $\langle D_i\rangle = U_i^\perp$. By Theorem 16, we have

$$\dim(\bigcap_{i=1}^t\langle H_1D_i\rangle) = \max_{P_1\sqcup\cdots\sqcup P_s=[t]}\left(\sum_{i=1}^s\dim(\bigcap_{j\in P_i}U_j^\perp) - (s-1)(n'-k)\right). \tag{16}$$

We proceed to compute the RHS of (16). For $s = 1$ and $P_1 = [t]$, as $\sum_{i\in[t]} U_i = \mathbb{F}_q^{n'}$, we conclude

$$\bigcap_{j\in[t]} U_i^{\perp} \overset{(1)}{=} (\sum_{i\in[t]} U_i)^{\perp} = 0. \tag{17}$$

For $s \geq 2$ and nonempty sets $P_1, \ldots, P_s$ that forms a partition of $[t]$, we have

$$\begin{aligned}\sum_{i=1}^{s} \dim(\bigcap_{j\in P_i} U_j) &\overset{(1)}{=} \sum_{i=1}^{s} \left(n' - \dim(\sum_{j\in P_i} U_j^{\perp})\right) = sn' + \sum_{i=1}^{s} \dim(\mathcal{U}_{P_i}) - \sum_{i=1}^{s}\sum_{j\in P_i} \dim(U_j) \\ &\overset{(14)}{\leq} sn' + (\lambda+1)\sum_{i=1}^{s}(|P_i|-1)k - \sum_{j=1}^{t} \dim(U_j) = sn' + (\lambda+1)k(t-s) - \dim(\mathcal{U}_{[t]}) - n' \\ &\overset{(13)}{\leq} sn' + (\lambda+1)k(t-s) - (1+\lambda)(t-1)k + \lambda k - n' \leq (s-1)(n'-k).\end{aligned} \tag{18}$$

Combining (16), (17), and (18), we conclude that $\bigcap_{i=1}^{t}\langle H_1 D_i\rangle = 0$. Now, by Lemma 9, this implies

$$\operatorname{rank}(M_{H,\mathcal{V}_{[t]}^{\perp}}) = \sum_{i=1}^{t} \dim(\langle HD_i\rangle) - \dim(\bigcap_{i=1}^{t}\langle H_1 D_i\rangle) = \sum_{i=1}^{t} \dim(\langle HD_i\rangle) = \sum_{i=1}^{t} \operatorname{rank}(D_i)$$

The last equality holds since by Lemma 8, the rank of $HD_i$ equals $\operatorname{rank}(D_i)$, as $D_i \subseteq \mathbb{F}_q^{n'\times\dim(U_i^{\perp})}$ is of full rank and $\dim(U_i^{\perp}) = n' - \dim(U_i) \leq n' - k$. Since the number of columns in $M_{H,\mathcal{V}_{[t]}^{\perp}}$ is $\sum_{i=1}^{t} \operatorname{rank}(D_i)$ which is equal to its rank, the only solution in $\ker(M_{H,\mathcal{V}_{[t]}^{\perp}})$ is 0. The proof is completed. ◀

## References


**1** Omar Alrabiah, Venkatesan Guruswami, and Ray Li. AG codes have no list-decoding friends: Approaching the generalized Singleton bound requires exponential alphabets. In *Proceedings of the 2024 Annual ACM-SIAM Symposium on Discrete Algorithms (SODA)*, pages 1367–1378. SIAM, 2024. doi:10.1137/1.9781611977912.55.

**2** Omar Alrabiah, Venkatesan Guruswami, and Ray Li. Randomly punctured Reed–Solomon codes achieve list-decoding capacity over linear-sized fields. In *Proceedings of the 56th Annual ACM Symposium on Theory of Computing*, pages 1458–1469, 2024. doi:10.1145/3618260.3649634.

**3** Hannes Bartz, Lukas Holzbaur, Hedongliang Liu, Sven Puchinger, Julian Renner, Antonia Wachter-Zeh, et al. Rank-metric codes and their applications. *Foundations and Trends® in Communications and Information Theory*, 19(3):390–546, 2022. doi:10.1561/0100000119.

**4** Joshua Brakensiek, Sivakanth Gopi, and Visu Makam. Lower bounds for maximally recoverable tensor codes and higher order MDS codes. *IEEE Transactions on Information Theory*, 68(11):7125–7140, 2022. doi:10.1109/TIT.2022.3187366.

**5** 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.

**6** Michael A. Forbes and Venkatesan Guruswami. Dimension Expanders via Rank Condensers. In *Approximation, Randomization, and Combinatorial Optimization. Algorithms and Techniques (APPROX/RANDOM 2015)*, pages 800–814, 2015. doi:10.4230/LIPIcs.APPROX-RANDOM.2015.800.

**7** Michael A Forbes and Amir Shpilka. On identity testing of tensors, low-rank recovery and compressed sensing. In *Proceedings of the forty-fourth annual ACM symposium on Theory of computing*, pages 163–172, 2012. doi:10.1145/2213977.2213995.

**8** Ernst Gabidulin. Theory of codes with maximum rank distance (translation). *Problems of Information Transmission*, 21:1–12, 01 1985.

**9** J. K. Gibson. Severely denting the Gabidulin version of the Mceliece public key cryptosystem. *Designs, Codes and Cryptography*, pages 37–45, 1995. doi:10.1007/BF01390769.

**10** J. K. Gibson. The security of the Gabidulin public-key cryptosystem. In *Advances in Cryptology – EUROCRYPT'96, LNCS 1070,*. Springer, 1996.

**11** Zeyu Guo, Ben Lee Volk, Akhil Jalan, and David Zuckerman. Extractors for images of varieties. In *Proceedings of the 55th Annual ACM Symposium on Theory of Computing*, pages 46–59, 2023. doi:10.1145/3564246.3585109.

**12** Zeyu Guo, Chaoping Xing, Chen Yuan, and Zihan Zhang. Random gabidulin codes achieve list decoding capacity in the rank metric. In *65th IEEE Annual Symposium on Foundations of Computer Science, FOCS 2024, Chicago, IL, USA, October 27-30, 2024*, pages 1846–1873. IEEE, 2024. doi:10.1109/FOCS61266.2024.00111.

**13** Zeyu Guo and Zihan Zhang. Randomly punctured Reed-Solomon codes achieve the list decoding capacity over polynomial-size alphabets. In *2023 IEEE 64th Annual Symposium on Foundations of Computer Science (FOCS)*, pages 164–176, 2023. doi:10.1109/FOCS57990.2023.00019.

**14** Venkatesan Guruswami, Nicolas Resch, and Chaoping Xing. Lossless dimension expanders via linearized polynomials and subspace designs. *Comb.*, 41(4):545–579, 2021. doi:10.1007/s00493-020-4360-1.

**15** 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.

**16** R. Koetter and F. R. Kschischang. Coding for errors and erasures in random network coding. In *IEEE International Symposium on Information Theory (ISIT 2007)*, pages 791–795. IEEE, 2007. doi:10.1109/ISIT.2007.4557321.

**17** 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.

**18** Pierre Loidreau. Designing a rank metric based mceliece cryptosystem. In *Post-Quantum Cryptography: Third International Workshop, PQCrypto 2010, Darmstadt, Germany, May 25-28, 2010. Proceedings 3*, pages 142–152. Springer, 2010. doi:10.1007/978-3-642-12929-2_11.

**19** Pierre Loidreau. A new rank metric codes based encryption scheme. In *Post-Quantum Cryptography: 8th International Workshop, PQCrypto 2017, Utrecht, The Netherlands, June 26-28, 2017, Proceedings 8*, pages 3–17. Springer, 2017. doi:10.1007/978-3-319-59879-6_1.

**20** Hsiao-feng Lu and P Vijay Kumar. A unified construction of space-time codes with optimal rate-diversity tradeoff. *IEEE Transactions on Information Theory*, 51(5):1709–1730, 2005. doi:10.1109/TIT.2005.846403.

**21** Paul Lusina, Ernst Gabidulin, and Martin Bossert. Maximum rank distance codes as space-time codes. *IEEE Transactions on Information Theory*, 49(10):2757–2760, 2003. doi:10.1109/TIT.2003.818023.

**22** Netanel Raviv and Antonia Wachter-Zeh. Some Gabidulin codes cannot be list decoded efficiently at any radius. *IEEE Transactions on Information Theory*, 62(4):1605–1615, 2016. doi:10.1109/TIT.2016.2532343.

**23** Netanel Raviv and Antonia Wachter-Zeh. A correction to "some Gabidulin codes cannot be list decoded efficiently at any radius". *IEEE Transactions on Information Theory*, 63(4):2623–2624, 2017. doi:10.1109/TIT.2017.2659766.

**24** Chong Shangguan and Itzhak Tamo. Combinatorial list-decoding of Reed-Solomon codes beyond the Johnson radius. In *Proceedings of the 52nd Annual ACM SIGACT Symposium on Theory of Computing*, pages 538–551, 2020. doi:10.1145/3357713.3384295.

**25** D. Silva and F. R. Kschischang. Fast encoding and decoding of Gabidulin codes. In *IEEE International Symposium on Information Theory (ISIT 2009)*. IEEE, 2009.

**26** D. Silva, F.R. Kschischang, and R. Koetter. A rank-metric approach to error control in random network coding. *IEEE Transactions on Information Theory*, 54(9):3951–3967, 2008. doi:10.1109/TIT.2008.928291.