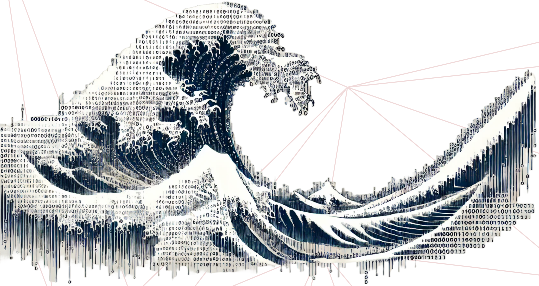


Zeyu Guo

zguotcs@gmail.com

Ohio State University

April 25, 2025

Random Gabidulin Codes Achieve List Decoding Capacity in the Rank Metric

joint work with Chaoping Xing (Shanghai Jiao Tong University), Chen Yuan (Shanghai Jiao Tong University), and Zihan Zhang (Ohio State University)

Introduction

Minimum Distance and Rate

An $[n,k]$ linear code C has two important parameters:

- Minimum distance: For a linear code C, $d_H(C) := \min\{w(y) : y \in C\}$.

Minimum Distance and Rate

An $[n,k]$ linear code C has two important parameters:

- Minimum distance: For a linear code C, $d_H(C) := \min\{w(y) : y \in C\}$.
- Rate: $R(C) = k/n$.

Minimum Distance and Rate

An $[n,k]$ linear code C has two important parameters:

- Minimum distance: For a linear code C, $d_H(C) := \min\{w(y) : y \in C\}$.
- Rate: $R(C) = k/n$.

Theorem (Singleton bound)

$d_H(C) \leq n - k + 1$.

Minimum Distance and Rate

An $[n,k]$ linear code C has two important parameters:

- Minimum distance: For a linear code C, $d_H(C) := \min\{w(y) : y \in C\}$.
- Rate: $R(C) = k/n$.

Theorem (Singleton bound)

$d_H(C) \le n - k + 1.$

- Optimal over sufficiently large fields.

Minimum Distance and Rate

An $[n,k]$ linear code C has two important parameters:

- Minimum distance: For a linear code C, $d_H(C) := \min\{w(y) : y \in C\}$.
- Rate: $R(C) = k/n$.

Theorem (Singleton bound)

$d_H(C) \leq n-k+1.$

- Optimal over sufficiently large fields.
- Achieved by codes such as Reed–Solomon codes.

Minimum Distance and Rate

An $[n,k]$ linear code C has two important parameters:

- Minimum distance: For a linear code C, $d_H(C) := \min\{w(y) : y \in C\}$.
- Rate: $R(C) = k/n$.

Theorem (Singleton bound)

$d_H(C) \leq n - k + 1.$

- Optimal over sufficiently large fields.
- Achieved by codes such as Reed–Solomon codes.
- Codes attaining the Singleton bound are called MDS codes.

Rank Codes: Matrix Formulation

- A rank code is a finite set C of $s \times n$ matrices over $\mathbb{F}_q$.

Rank Codes: Matrix Formulation

- A rank code is a finite set C of $s \times n$ matrices over $\mathbb{F}_q$.
- It uses the rank distance d_R instead of the Hamming distance d_H:

$$d_R(M_1, M_2) := \mathrm{rank}(M_1 - M_2).$$

Rank Codes: Matrix Formulation

- A rank code is a finite set C of $s \times n$ matrices over $\mathbb{F}_q$.
- It uses the rank distance d_R instead of the Hamming distance d_H:

$$d_R(M_1, M_2) := \operatorname{rank}(M_1 - M_2).$$

- The Singleton bound also holds with respect to the rank metric.

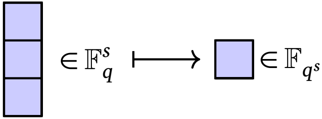
Rank Codes: Vector Formulation

Rank Codes: Vector Formulation

Fix a bijective $\mathbb{F}_q$-linear map $\mathbb{F}_q^s \to \mathbb{F}_{q^s}$.

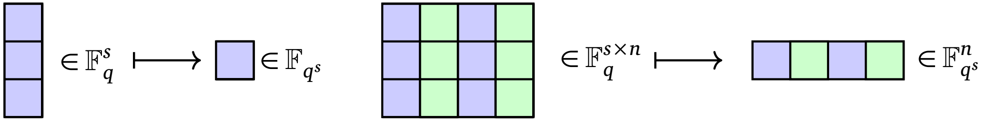
Rank Codes: Vector Formulation

Fix a bijective $\mathbb{F}_q$-linear map $\mathbb{F}_q^s \to \mathbb{F}_{q^s}$.



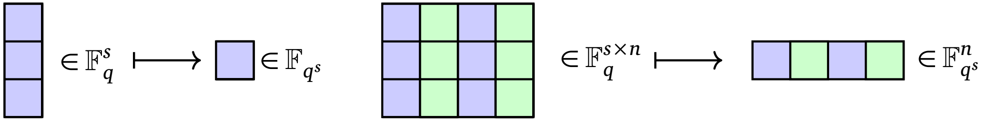
Rank Codes: Vector Formulation

Fix a bijective $\mathbb{F}_q$-linear map $\mathbb{F}_q^s \to \mathbb{F}_{q^s}$.



Rank Codes: Vector Formulation

Fix a bijective $\mathbb{F}_q$-linear map $\mathbb{F}_q^s \to \mathbb{F}_{q^s}$.



Remark

$d_R(x,y) \le d_H(x,y)$.

Remark

$d_R(x,y) \leq d_H(x,y)$.

Remark

$d_R(x, y) \leq d_H(x, y)$.

Corollary (Singleton bound)

$d_R(C) \leq n - k + 1$ for an $[n, k]$ linear rank code C over $\mathbb{F}_{q^s}$.

Rank Codes: Vector Formulation

Remark

$d_R(x, y) \leq d_H(x, y)$.

Corollary (Singleton bound)

$d_R(C) \leq n - k + 1$ *for an* $[n, k]$ *linear rank code* C *over* $\mathbb{F}_{q^s}$.

Rank codes achieving this bound are called Maximum Rank Distance (MRD) codes.

Rank Codes: Vector Formulation

Remark

$d_R(x, y) \le d_H(x, y)$.

Corollary (Singleton bound)

$d_R(C) \le n - k + 1$ for an $[n, k]$ linear rank code C over $\mathbb{F}_{q^s}$.

Rank codes achieving this bound are called Maximum Rank Distance (MRD) codes.

Corollary

All MRD codes are MDS codes.

Definition (Linearized polynomials)

Let q be a prime power. We say $f(x)$ is q-linearized if it has the form

$$f(x) = a_d x^{q^d} + a_{d-1} x^{q^{d-1}} + \cdots + a_1 x^q + a_0 x.$$

Definition (Linearized polynomials)

Let q be a prime power. We say $f(x)$ is q-linearized if it has the form

$$f(x) = a_d x^{q^d} + a_{d-1} x^{q^{d-1}} + \cdots + a_1 x^q + a_0 x.$$

where $\deg_q(f) := d$ is called the q-degree of f.

Linearized Polynomials

Definition (Linearized polynomials)

Let q be a prime power. We say $f(x)$ is q-linearized if it has the form

$$f(x) = a_d x^{q^d} + a_{d-1} x^{q^{d-1}} + \cdots + a_1 x^q + a_0 x.$$

where $\deg_q(f) := d$ is called the q-degree of f.

- The composition of two q-linearized polynomial is again a q-linearized polynomial.

Definition (Linearized polynomials)

Let q be a prime power. We say $f(x)$ is q-linearized if it has the form

$$f(x) = a_d x^{q^d} + a_{d-1} x^{q^{d-1}} + \cdots + a_1 x^q + a_0 x.$$

where $\deg_q(f) := d$ is called the q-degree of f.

- The composition of two q-linearized polynomial is again a q-linearized polynomial.
- Composition is generally noncommutative: $(cX) \circ (X^q) = cX^q$ while $(X^q) \circ (cX) = c^q X^q$.

Definition (Gabidulin codes)

Given $\alpha_1, \alpha_2, \dots, \alpha_n \in \mathbb{F}_{q^s}$ that are linearly independent over $\mathbb{F}_q$, the corresponding $[n,k]$ Gabidulin code is

$$\mathsf{G}_{n,k}(\alpha_1, \dots, \alpha_n) := \left\{ \big(f(\alpha_1), \dots, f(\alpha_n)\big) \;\middle|\; \begin{array}{l} q\text{-linearized } f \in \mathbb{F}_{q^s}[x], \\ \deg_q(f) < k \end{array} \right\} \subseteq \mathbb{F}_{q^s}^n .$$

Definition (Gabidulin codes)

Given $\alpha_1, \alpha_2, \ldots, \alpha_n \in \mathbb{F}_{q^s}$ that are linearly independent over $\mathbb{F}_q$, the corresponding $[n,k]$ Gabidulin code is

$$\mathsf{G}_{n,k}(\alpha_1, \ldots, \alpha_n) := \left\{ \big(f(\alpha_1), \ldots, f(\alpha_n)\big) \;\middle|\; \begin{array}{l} q\text{-linearized } f \in \mathbb{F}_{q^s}[x], \\ \deg_q(f) < k \end{array} \right\} \subseteq \mathbb{F}_{q^s}^n.$$

Theorem

Gabidulin codes are MRD codes.

Why Care About Rank Codes and Gabidulin Codes?

Why Care About Rank Codes and Gabidulin Codes?

- Useful for error and erasure correction in network coding (e.g., [Koetter–Kschischang ’08], [Silva–Koetter–Kschischang ’08]).

Why Care About Rank Codes and Gabidulin Codes?

- Useful for error and erasure correction in network coding (e.g., [Koetter–Kschischang '08], [Silva–Koetter–Kschischang '08]).
- Applied in constructing public-key cryptosystems (e.g., [Chabaud–Stern '96], [Loidreau '10]).

Why Care About Rank Codes and Gabidulin Codes?

- Useful for error and erasure correction in network coding (e.g., [Koetter–Kschischang '08], [Silva–Koetter–Kschischang '08]).
- Applied in constructing public-key cryptosystems (e.g., [Chabaud–Stern '96], [Loidreau '10]).
- Connected with two-source rank condensers [Forbes–Guruswami '14], dimension expanders [Guruswami–Resch–Xing '18], and deterministic extractors [Guo–Volk–Jalan–Zuckerman '23].

List Decodability

Combinatorial List Decodability

Definition (Combinatorial list decodability)

For $\rho \in [0,1]$ and $L \geq 1$, a code $C \subseteq \mathbb{F}_q^n$ is (ρ, L) list decodable if for all $y \in \mathbb{F}_q^n$ and $L+1$ distinct codewords $c_0, c_1, \ldots, c_L \in C$,

$$\max_{0 \leq i \leq L} d(y, c_i) > \rho n.$$

Combinatorial List Decodability

Definition (Combinatorial list decodability)

For $\rho \in [0,1]$ and $L \geq 1$, a code $C \subseteq \mathbb{F}_q^n$ is (ρ, L) list decodable if for all $y \in \mathbb{F}_q^n$ and $L+1$ distinct codewords $c_0, c_1, \ldots, c_L \in C$,

$$\max_{0 \leq i \leq L} d(y, c_i) > \rho n.$$

Definition (Average-radius combinatorial list decodability)

For $\rho \in [0,1]$ and $L \geq 1$, a code $C \subseteq \mathbb{F}_q^n$ is (ρ, L) average-radius list decodable if for all $y \in \mathbb{F}_q^n$ and $L+1$ distinct codewords $c_0, c_1, \ldots, c_L \in C$,

$$\frac{1}{L+1} \sum_{i=0}^{L} d(y, c_i) > \rho n.$$

Combinatorial List Decodability of RS Codes in Hamming Metric

Theorem (Johnson Bound)

Any $[n,k]$ *code* C *with distance* $d(C)$ *is* $\left(1-\sqrt{1-\frac{d(C)}{n}}, qnd(C)\right)$ *list decodable in the Hamming metric.*

Combinatorial List Decodability of RS Codes in Hamming Metric

Theorem (Johnson Bound)

Any $[n,k]$ *code* C *with distance* $d(C)$ *is* $\left(1-\sqrt{1-\frac{d(C)}{n}}, qnd(C)\right)$ *list decodable in the Hamming metric.*

Corollary

Any $[n,k]$ *RS code* C *of rate* R *over* $\mathbb{F}_q$ *is* $\left(1-\sqrt{R}, L\right)$ *list decodable in the Hamming metric, where* $L = qnd(C)$.

Combinatorial List Decodability of Gabidulin Codes in Rank Metric

List decoding Gabidulin codes in the **rank metric** is more challenging:

- There is no Johnson bound in the rank metric [Wachter-Zeh '13].

Combinatorial List Decodability of Gabidulin Codes in Rank Metric

List decoding Gabidulin codes in the **rank metric** is more challenging:

- There is no Johnson bound in the rank metric [Wachter-Zeh '13].
- There exist Gabidulin codes that are not list decodable beyond the unique decoding radius [Raviv–Wachter-Zeh '15].

Combinatorial List Decodability of Gabidulin Codes in Rank Metric

List decoding Gabidulin codes in the **rank metric** is more challenging:

- There is no Johnson bound in the rank metric [Wachter-Zeh '13].
- There exist Gabidulin codes that are not list decodable beyond the unique decoding radius [Raviv–Wachter-Zeh '15].

What about a random Gabidulin code $\mathsf{G}_{n,k}(\alpha_1, \ldots, \alpha_n)$?

Generalized Singleton Bound

Theorem (Generalized Singleton Bound [Shangguan–Tamo '20])

If a linear code C of rate R is (ρ, L) list decodable in the Hamming metric, then

$$\rho \leq \frac{L}{L+1}(1-R).$$

Theorem (Generalized Singleton Bound [Shangguan–Tamo '20])

If a linear code C of rate R is (ρ, L) list decodable in the Hamming metric, then

$$\rho \leq \frac{L}{L+1}(1-R).$$

Theorem ([Brakensiek–Gopi–Makam '23])

For any L, a random Reed–Solomon code of rate R over a sufficiently large field is, w.h.p, $\left(\frac{L}{L+1}(1-R), L\right)$ average-radius list decodable in the Hamming metric.

Theorem (Generalized Singleton Bound [Shangguan–Tamo '20])

If a linear code C of rate R is (ρ, L) list decodable in the Hamming metric, then

$$\rho \leq \frac{L}{L+1}(1-R).$$

Theorem ([Brakensiek–Gopi–Makam '23])

For any L, a random Reed–Solomon code of rate R over a sufficiently large field is, w.h.p, $\left(\frac{L}{L+1}(1-R), L\right)$ average-radius list decodable in the Hamming metric.

We show that random Gabidulin codes (over sufficiently large fields) achieve the generalized Singleton bound, even in the rank metric.

Higher Order MDS Codes

Theorem ([Brakensiek–Gopi–Makam '23])

For any L, a random Reed–Solomon code of rate R over a sufficiently large field is, w.h.p, $\left(\frac{L}{L+1}(1-R), L\right)$ average-radius list decodable.

Higher Order MDS Codes

Theorem ([Brakensiek–Gopi–Makam '23])

For any L, a random Reed–Solomon code of rate R over a sufficiently large field is, w.h.p, $\left(\frac{L}{L+1}(1-R), L\right)$ average-radius list decodable.

- Brakensiek–Gopi–Makam '23 introduced three notions of "higher order MDS codes": $\mathrm{MDS}(L)$, $\mathrm{GZP}(L)$, and $\mathrm{LD\text{-}MDS}(L)$ for each $L \geq 1$.

Theorem ([Brakensiek–Gopi–Makam '23])

For any L, a random Reed–Solomon code of rate R over a sufficiently large field is, w.h.p, $\left(\frac{L}{L+1}(1-R), L\right)$ average-radius list decodable.

- Brakensiek–Gopi–Makam '23 introduced three notions of "higher order MDS codes": $\mathrm{MDS}(L)$, $\mathrm{GZP}(L)$, and $\text{LD-MDS}(L)$ for each $L \geq 1$.
- C is $\text{LD-MDS}(L)$ if it is $\left(\frac{L}{L+1}(1-R), L\right)$ average-radius list decodable.

Theorem ([Brakensiek–Gopi–Makam ’23])

For any L, a random Reed–Solomon code of rate R over a sufficiently large field is, w.h.p, $\left(\frac{L}{L+1}(1-R), L\right)$ average-radius list decodable.

- Brakensiek–Gopi–Makam ’23 introduced three notions of “higher order MDS codes”: $\mathrm{MDS}(L)$, $\mathrm{GZP}(L)$, and $\text{LD-MDS}(L)$ for each $L \geq 1$.
- C is $\text{LD-MDS}(L)$ if it is $\left(\frac{L}{L+1}(1-R), L\right)$ average-radius list decodable.
- Brakensiek et al. proved that these notions are equivalent up to duality.

Higher Order MDS Codes

Theorem ([Brakensiek–Gopi–Makam ’23])

For any L, a random Reed–Solomon code of rate R over a sufficiently large field is, w.h.p, $\left(\frac{L}{L+1}(1-R), L\right)$ *average-radius list decodable.*

- Brakensiek–Gopi–Makam ’23 introduced three notions of “higher order MDS codes”: $\mathrm{MDS}(L)$, $\mathrm{GZP}(L)$, and $\text{LD-MDS}(L)$ for each $L \geq 1$.
- C is $\text{LD-MDS}(L)$ if it is $\left(\frac{L}{L+1}(1-R), L\right)$ average-radius list decodable.
- Brakensiek et al. proved that these notions are equivalent up to duality.

$$\begin{tikzcd}
 & C \text{ is } \mathrm{MDS}(L+1) \arrow[dl, Leftrightarrow] \arrow[dr, Leftrightarrow] & \\
C \text{ is } \mathrm{GZP}(L+1) \arrow[rr, Leftrightarrow] & & \begin{array}{c} C^{\perp} \text{ is } \text{LD-MDS}(L') \\ \text{for all } L' \leq L \end{array}
\end{tikzcd}$$

Theorem (GM-MDS Theorem [Lovett '18, Yildiz–Hassibi '18])

Random RS codes over large enough fields are w.h.p. GZP(L) for all $L \geq 1$.

Theorem (GM-MDS Theorem [Lovett '18, Yildiz–Hassibi '18])

Random RS codes over large enough fields are w.h.p. GZP(L) for all $L \geq 1$.

- Combining this with

GM-MDS Theorem

Theorem (GM-MDS Theorem [Lovett '18, Yildiz–Hassibi '18])

Random RS codes over large enough fields are w.h.p. GZP(L) for all $L \geq 1$.

- Combining this with
  - the equivalence among higher order MDS codes (up to duality), and

Theorem (GM-MDS Theorem [Lovett '18, Yildiz–Hassibi '18])

Random RS codes over large enough fields are w.h.p. GZP(L) for all $L \geq 1$.

- Combining this with
  - the equivalence among higher order MDS codes (up to duality), and
  - the fact that the dual code of an RS code is also an RS code up to scaling of coordinates

Theorem (GM-MDS Theorem [Lovett '18, Yildiz–Hassibi '18])

Random RS codes over large enough fields are w.h.p. GZP(L) for all $L \geq 1$.

- Combining this with
  - the equivalence among higher order MDS codes (up to duality), and
  - the fact that the dual code of an RS code is also an RS code up to scaling of coordinates

  proves the main result of [Brakensiek–Gopi–Makam '23].

Our Results

Combinatorial List Decodability of Random Gabidulin Codes

Theorem (Guo–Xing–Yuan–Zhang '24)

For any $L \geq 1$, a random Gabidulin code of rate R over a sufficiently large field is, w.h.p, $\left(\frac{L}{L+1}(1-R), L\right)$ average-radius list decodable in the rank metric.

Combinatorial List Decodability of Random Gabidulin Codes

Theorem (Guo–Xing–Yuan–Zhang '24)

For any $L \geq 1$, a random Gabidulin code of rate R over a sufficiently large field is, w.h.p, $\left(\frac{L}{L+1}(1-R), L\right)$ average-radius list decodable in the rank metric.

To prove the theorem, we develop a theory of "higher-order MRD codes" for rank codes, analogous to the theory of higher-order MDS codes developed by Brakensiek, Gopi, and Makam.

Higher Order MRD Codes

- We introduce an analogous theory by introducing three notions of "higher order MRD codes": $\mathrm{MRD}(L)$, $\mathrm{GKP}(L)$, and $\mathrm{LD\text{-}MRD}(L)$.

Higher Order MRD Codes

- We introduce an analogous theory by introducing three notions of "higher order MRD codes": $\mathrm{MRD}(L)$, $\mathrm{GKP}(L)$, and $\mathrm{LD\text{-}MRD}(L)$.
- C is $\mathrm{LD\text{-}MRD}(L)$ if it is $\left(\frac{L}{L+1}(1-R), L\right)$ average-radius list decodable in the rank metric.

Higher Order MRD Codes

- We introduce an analogous theory by introducing three notions of "higher order MRD codes": MRD(L), GKP(L), and LD-MRD(L).
- C is LD-MRD(L) if it is $\left(\frac{L}{L+1}(1-R), L\right)$ average-radius list decodable in the rank metric.
- We further proved that these notions are equivalent up to duality.

Higher Order MRD Codes

- We introduce an analogous theory by introducing three notions of "higher order MRD codes": MRD(L), GKP(L), and LD-MRD(L).
- C is LD-MRD(L) if it is $\left(\frac{L}{L+1}(1-R), L\right)$ average-radius list decodable in the rank metric.
- We further proved that these notions are equivalent up to duality.

$$\begin{tikzcd} & C \text{ is } \mathrm{MRD}(L+1) \arrow[dl, Leftrightarrow] \arrow[dr, Leftrightarrow] & \\ C \text{ is } \mathrm{GKP}(L+1) \arrow[rr, Leftrightarrow] & & \begin{array}{c} C^{\perp} \text{ is LD-MRD}(L') \\ \text{for all } L' \le L \end{array} \end{tikzcd}$$

GM-MRD Theorem

Furthermore, we prove an analogy of the GM-MDS Theorem.

Furthermore, we prove an analogy of the GM-MDS Theorem.

Theorem (GM-MRD Theorem [Guo–Xing–Yuan–Zhang '24])

Random Gabilidulin codes over large enough fields are w.h.p. GKP(L) for all $L \geq 1$.

Furthermore, we prove an analogy of the GM-MDS Theorem.

Theorem (GM-MRD Theorem [Guo–Xing–Yuan–Zhang '24])

Random Gabilidulin codes over large enough fields are w.h.p. GKP(L) for all $L \geq 1$.

Fact

The dual of a Gabidulin code is also a Gabidulin code.

GM-MRD Theorem

Furthermore, we prove an analogy of the GM-MDS Theorem.

Theorem (GM-MRD Theorem [Guo–Xing–Yuan–Zhang ’24])

Random Gabilidulin codes over large enough fields are w.h.p. GKP(L) for all $L \geq 1$.

Fact

The dual of a Gabidulin code is also a Gabidulin code.

Combining the GM-MRD theorem, the equivalence among higher order MRD codes, and the fact that Gabidulin codes are self-dual, we obtain:

GM-MRD Theorem

Furthermore, we prove an analogy of the GM-MDS Theorem.

Theorem (GM-MRD Theorem [Guo–Xing–Yuan–Zhang '24])

Random Gabilidulin codes over large enough fields are w.h.p. GKP(L) for all $L \geq 1$.

Fact

The dual of a Gabidulin code is also a Gabidulin code.

Combining the GM-MRD theorem, the equivalence among higher order MRD codes, and the fact that Gabidulin codes are self-dual, we obtain:

Corollary ([Guo–Xing–Yuan–Zhang '24])

For all $L \geq 1$, *random Gabidulin codes of rate* R *over large enough fields are w.h.p.* $\left(\frac{L}{L+1}(1-R), L\right)$ *average-radius list decodable in the rank metric.*

An Interesting Formula for Generic Intersections

Generic Intersection Formula

Definition

For symbolic (generic) matrix $W = \left(X_{ij}\right) \in \mathbb{F}_q(X_{11}, \cdots, X_{kn})^{k \times n}$ and a set $A \subseteq [n]$, define the subspace

$$W_A := \operatorname{span}_{\mathbb{F}_q(X_{11},\cdots,X_{kn})}\{i\text{-th column vector of } W : i \in A\} \subseteq \mathbb{F}_q(X_{11}, \cdots, X_{kn})^k.$$

Generic Intersection Formula

Definition

For symbolic (generic) matrix $W = \left(X_{ij}\right) \in \mathbb{F}_q(X_{11}, \cdots, X_{kn})^{k \times n}$ and a set $A \subseteq [n]$, define the subspace

$$W_A := \operatorname{span}_{\mathbb{F}_q(X_{11},\cdots,X_{kn})}\{i\text{-th column vector of } W : i \in A\} \subseteq \mathbb{F}_q(X_{11}, \cdots, X_{kn})^k.$$

Theorem (Generic Intersection Formula [Brakensiek–Gopi–Makam '23])

Given $A_1, \ldots, A_\ell \subseteq [n]$ of size at most k, for a $k \times n$ generic matrix W,

$$\dim\left(W_{A_1} \cap \cdots \cap W_{A_\ell}\right) = \max_{P_1 \sqcup P_2 \sqcup \cdots \sqcup P_s = [\ell]} \left(\sum_{i \in [s]} \left| \bigcap_{j \in P_i} A_j \right| - (s-1)k \right).$$

Generic Intersection Formula: A Generalization

Definition

For symbolic (generic) matrix $W = \left(X_{ij}\right) \in \mathbb{F}_q(X_{11}, \cdots, X_{kn})^{k\times n}$ and a subspace $V \subseteq \mathbb{F}_q^n$, define the subspace

$$W_V := \mathrm{span}_{\mathbb{F}_q(X_{11},\cdots,X_{kn})}\{W \cdot \vec{v} \text{ for } \vec{v} \in V\} \subseteq \mathbb{F}_q(X_{11}, \cdots, X_{kn})^k.$$

Generic Intersection Formula: A Generalization

Definition

For symbolic (generic) matrix $W = \left(X_{ij}\right) \in \mathbb{F}_q(X_{11}, \cdots, X_{kn})^{k\times n}$ and a subspace $V \subseteq \mathbb{F}_q^n$, define the subspace

$$W_V := \mathrm{span}_{\mathbb{F}_q(X_{11},\cdots,X_{kn})}\{W\cdot\vec{v} \text{ for } \vec{v}\in V\} \subseteq \mathbb{F}_q(X_{11},\cdots,X_{kn})^k.$$

Theorem ([Guo–Xing–Yuan–Zhang '24])

Given $V_1,\ldots,V_\ell \subseteq \mathbb{F}_q^n$ of dimension at most k, for a $k\times n$ generic matrix W,

$$\dim\left(W_{V_1}\cap\cdots\cap W_{V_\ell}\right) = \max_{P_1\sqcup P_2\sqcup\cdots\sqcup P_s=[\ell]}\left(\sum_{i\in[s]}\dim_{\mathbb{F}_q}\left(\bigcap_{j\in P_i}V_j\right) - (s-1)k\right).$$

Related Works

Reducing the Alphabet Size

Theorem (Guo–Xing–Yuan–Zhang '24)

For any $L \geq 1$, a random Gabidulin code of rate R over a sufficiently large field is, w.h.p, $\left(\frac{L}{L+1}(1-R), L\right)$ average-radius list decodable in the rank metric.

Reducing the Alphabet Size

Theorem (Guo–Xing–Yuan–Zhang '24)

For any $L \geq 1$, a random Gabidulin code of rate R over a sufficiently large field is, w.h.p, $\left(\frac{L}{L+1}(1-R), L\right)$ average-radius list decodable in the rank metric.

- It suffices to choose the alphabet size q^s with $s = O_L(nk)$.

Theorem (Guo–Xing–Yuan–Zhang '24)

For any $L \geq 1$, a random Gabidulin code of rate R over a sufficiently large field is, w.h.p, $\left(\frac{L}{L+1}(1-R), L\right)$ average-radius list decodable in the rank metric.

- It suffices to choose the alphabet size q^s with $s = O_L(nk)$.
- In a follow-up paper, we reduce the alphabet size.

Reducing the Alphabet Size

Theorem (Guo–Xing–Yuan–Zhang '24)

For any $L \geq 1$, a random Gabidulin code of rate R over a sufficiently large field is, w.h.p, $\left(\frac{L}{L+1}(1-R), L\right)$ average-radius list decodable in the rank metric.

- It suffices to choose the alphabet size q^s with $s = O_L(nk)$.
- In a follow-up paper, we reduce the alphabet size.

Theorem (Guo–Xing–Yuan–Zhang)

For any $L \geq 1$, a random Gabidulin code of rate R over a field of size $q^s = q^{O_{L,\varepsilon}(n)}$ is, w.h.p, $\left(\frac{L}{L+1}(1-R-\varepsilon), L\right)$ average-radius list decodable in the rank metric.

Reducing the Alphabet Size

Theorem (Guo–Xing–Yuan–Zhang '24)

For any $L \geq 1$, a random Gabidulin code of rate R over a sufficiently large field is, w.h.p, $\left(\frac{L}{L+1}(1-R), L\right)$ average-radius list decodable in the rank metric.

- It suffices to choose the alphabet size q^s with $s = O_L(nk)$.
- In a follow-up paper, we reduce the alphabet size.

Theorem (Guo–Xing–Yuan–Zhang)

For any $L \geq 1$, a random Gabidulin code of rate R over a field of size $q^s = q^{O_{L,\varepsilon}(n)}$ is, w.h.p, $\left(\frac{L}{L+1}(1-R-\varepsilon), L\right)$ average-radius list decodable in the rank metric.

- Analogous to [Guo–Zhang '23] and [Alrabiah–Guruswami–Li '23].

Explicit Rank Codes Achieving Singleton Bound

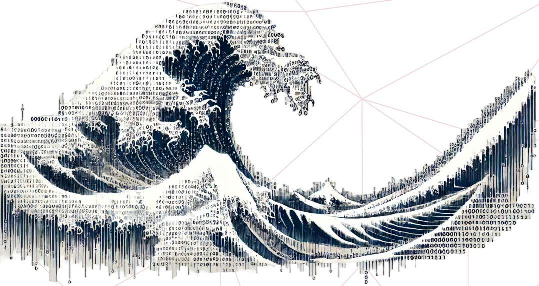
- [Mahdavifar–Vardy '12] defined *folded Gabidulin codes* and showed that they achieve the Singleton bound $1-R-\varepsilon$ in the rank metric. However, the rate R in their result approaches zero.

Explicit Rank Codes Achieving Singleton Bound

- [Mahdavifar–Vardy '12] defined *folded Gabidulin codes* and showed that they achieve the Singleton bound $1-R-\varepsilon$ in the rank metric. However, the rate R in their result approaches zero.
- [Guruswami–Xing '12] gave a Monte-Carlo construction of subcodes of folded Gabidulin codes that are $(1-R-\varepsilon, O(1/\varepsilon))$ list decodable in the rank metric.

Explicit Rank Codes Achieving Singleton Bound

- [Mahdavifar–Vardy '12] defined *folded Gabidulin codes* and showed that they achieve the Singleton bound $1-R-\varepsilon$ in the rank metric. However, the rate R in their result approaches zero.
- [Guruswami–Xing '12] gave a Monte-Carlo construction of subcodes of folded Gabidulin codes that are $(1-R-\varepsilon, O(1/\varepsilon))$ list decodable in the rank metric.
- [Guruswami–Wang–Xing '16] gave an explicit construction of subcodes of folded Gabidulin codes that are $(1-R-\varepsilon, (1/\varepsilon)^{O(1/\varepsilon)})$ list decodable in the rank metric.



The End