



Bounds on List Decoding of Rank-Metric Codes

Antonia Wachter-Zeh

Computer Science Department, Technion—Israel Institute of Technology

November 3, 2013

Motivation: Network Coding

$x_0=10000$ ← packet 0

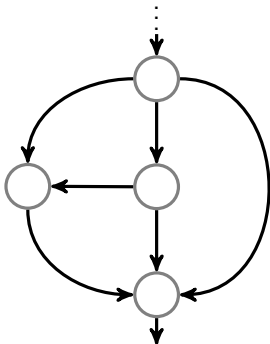
$x_1=10100$ ← packet 1

$x_2=01001$ ← packet 2

⋮

Motivation: Network Coding

$x_0=10000$ ← packet 0
 $x_1=10100$ ← packet 1
 $x_2=01001$ ← packet 2

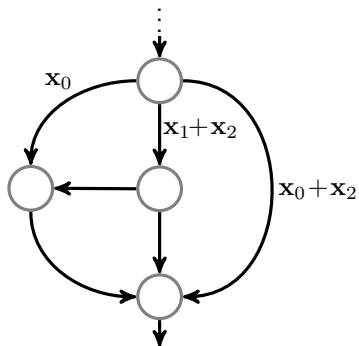


Motivation: Network Coding

$x_0=10000$ ← packet 0

$x_1=10100$ ← packet 1

$x_2=01001$ ← packet 2

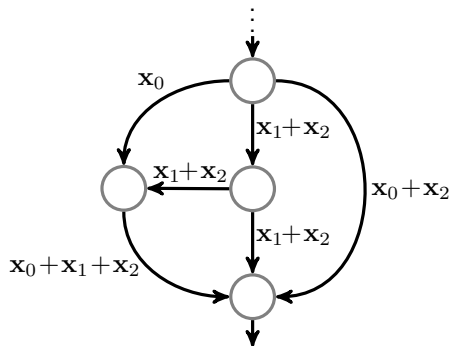


Motivation: Network Coding

$x_0=10000$ ← packet 0

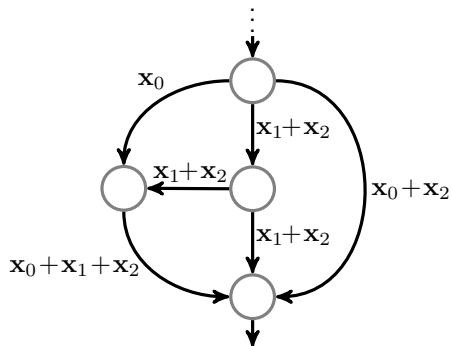
$x_1=10100$ ← packet 1

$x_2=01001$ ← packet 2



Motivation: Network Coding

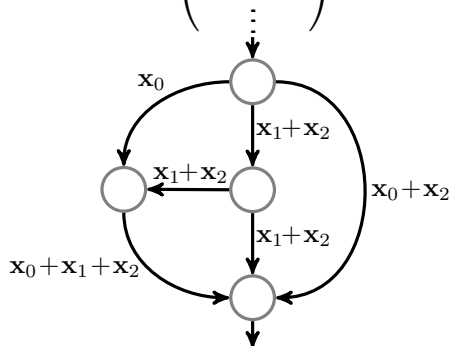
$x_0=10000$ ← packet 0
 $x_1=10100$ ← packet 1
 $x_2=01001$ ← packet 2



$x_0+x_1+x_2=01101$
 $x_0+x_1=00100$
 $x_0+x_2=11001$
⋮

Motivation: Network Coding

$$\mathbf{X} = \begin{pmatrix} \mathbf{x}_0=10000 \\ \mathbf{x}_1=10100 \\ \mathbf{x}_2=01001 \\ \vdots \end{pmatrix} \begin{array}{l} \leftarrow \text{packet 0} \\ \leftarrow \text{packet 1} \\ \leftarrow \text{packet 2} \end{array}$$

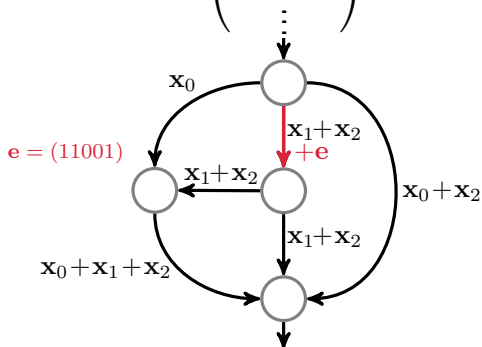


$$\mathbf{Y} = \begin{pmatrix} \mathbf{x}_0 + \mathbf{x}_1 + \mathbf{x}_2 = 01101 \\ \mathbf{x}_0 + \mathbf{x}_1 = 00100 \\ \mathbf{x}_0 + \mathbf{x}_2 = 11001 \\ \vdots \end{pmatrix}$$

- error-free:
 $\text{rowspace}(\mathbf{X}) = \text{rowspace}(\mathbf{Y})$

Motivation: Network Coding

$$\mathbf{X} = \begin{pmatrix} \mathbf{x}_0=10000 \\ \mathbf{x}_1=10100 \\ \mathbf{x}_2=01001 \\ \vdots \end{pmatrix} \begin{array}{l} \leftarrow \text{packet 0} \\ \leftarrow \text{packet 1} \\ \leftarrow \text{packet 2} \end{array}$$

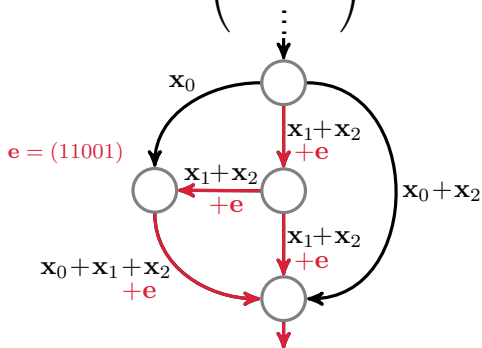


$$\mathbf{Y} = \begin{pmatrix} \mathbf{x}_0 + \mathbf{x}_1 + \mathbf{x}_2 = 01101 \\ \mathbf{x}_0 + \mathbf{x}_1 = 00100 \\ \mathbf{x}_0 + \mathbf{x}_2 = 11001 \\ \vdots \end{pmatrix}$$

- error-free:
 $\text{rowspace}(\mathbf{X}) = \text{rowspace}(\mathbf{Y})$

Motivation: Network Coding

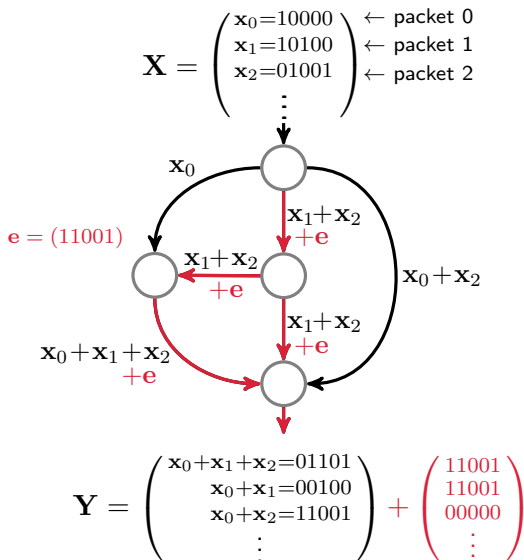
$$\mathbf{X} = \begin{pmatrix} x_0=10000 \\ x_1=10100 \\ x_2=01001 \\ \vdots \end{pmatrix} \begin{array}{l} \leftarrow \text{packet 0} \\ \leftarrow \text{packet 1} \\ \leftarrow \text{packet 2} \end{array}$$



$$\mathbf{Y} = \begin{pmatrix} x_0+x_1+x_2=01101 \\ x_0+x_1=00100 \\ x_0+x_2=11001 \\ \vdots \end{pmatrix} + \begin{pmatrix} 11001 \\ 11001 \\ 00000 \\ \vdots \end{pmatrix}$$

- error-free:
 $\text{rowspace}(\mathbf{X}) = \text{rowspace}(\mathbf{Y})$

Motivation: Network Coding



- error-free:
 $\text{rowspace}(\mathbf{X}) = \text{rowspace}(\mathbf{Y})$
- rank of **error** small

*Silva, Kötter,
Kschischang (2008)*
 \implies use subspace &
 rank-metric codes

- 1 Rank-Metric Codes & Decoding Principles
- 2 Problem Statement
- 3 Bound on the List Size of Gabidulin Codes
 - Lower Bound
 - Asymptotic Behavior of Bounds
- 4 Bounds for Rank-Metric Codes
 - Interpretation as Constant-Rank Code
 - Upper Bound
 - Lower Bound
 - Asymptotic Behavior of Bounds
- 5 Conclusion & Outlook

- 1 Rank-Metric Codes & Decoding Principles
- 2 Problem Statement
- 3 Bound on the List Size of Gabidulin Codes
 - Lower Bound
 - Asymptotic Behavior of Bounds
- 4 Bounds for Rank-Metric Codes
 - Interpretation as Constant-Rank Code
 - Upper Bound
 - Lower Bound
 - Asymptotic Behavior of Bounds
- 5 Conclusion & Outlook

Rank Metric

- bijective map $\mathbf{x} \in \mathbb{F}_{q^m}^n \mapsto \mathbf{X} \in \mathbb{F}_q^{m \times n}$
- rank norm: $\text{rk}(\mathbf{x}) \stackrel{\text{def}}{=} \text{rank of } \mathbf{X} \text{ over } \mathbb{F}_q$

minimum rank distance of an $(n, M, d)_R$ code \mathbf{C} over \mathbb{F}_{q^m} :

- $d \stackrel{\text{def}}{=} \min \{ \text{rk}(\mathbf{a} - \mathbf{b}) : \mathbf{a}, \mathbf{b} \in \mathbf{C}, \mathbf{a} \neq \mathbf{b} \}$
- $M \leq q^{\min\{n(m-d+1), m(n-d+1)\}}$
- equality: MRD code

Linearized Polynomial over \mathbb{F}_{q^m}

- $f(x) \stackrel{\text{def}}{=} \sum_{i=0}^{d_f} f_i x^{[i]} = \sum_{i=0}^{d_f} f_i x^{q^i}$ with $f_i \in \mathbb{F}_{q^m}$
- q -degree: $\deg_q f(x) = d_f$

Rank Metric

- bijective map $\mathbf{x} \in \mathbb{F}_{q^m}^n \mapsto \mathbf{X} \in \mathbb{F}_q^{m \times n}$
- rank norm: $\text{rk}(\mathbf{x}) \stackrel{\text{def}}{=} \text{rank of } \mathbf{X} \text{ over } \mathbb{F}_q$

minimum rank distance of an $(n, M, d)_R$ code \mathbf{C} over \mathbb{F}_{q^m} :

- $d \stackrel{\text{def}}{=} \min \{ \text{rk}(\mathbf{a} - \mathbf{b}) : \mathbf{a}, \mathbf{b} \in \mathbf{C}, \mathbf{a} \neq \mathbf{b} \}$
- $M \leq q^{\min\{n(m-d+1), m(n-d+1)\}}$
- equality: MRD code

Linearized Polynomial over \mathbb{F}_{q^m}

- $f(x) \stackrel{\text{def}}{=} \sum_{i=0}^{d_f} f_i x^{[i]} = \sum_{i=0}^{d_f} f_i x^{q^i}$ with $f_i \in \mathbb{F}_{q^m}$
- q -degree: $\deg_q f(x) = d_f$

Introduced by *Delsarte* (1978), *Gabidulin* (1985), *Roth* (1991)

Definition (Gabidulin Code)

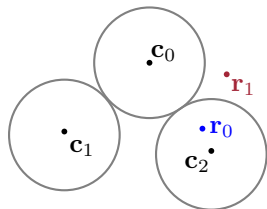
A linear **Gabidulin code** over \mathbb{F}_{q^m} of length $n \leq m$ and dimension $k \leq n$ is defined by

$$\text{Gab}[n, k] \stackrel{\text{def}}{=} \{ (f(g_0) \ f(g_1) \ \dots \ f(g_{n-1})) : \deg_q f(x) < k \},$$

where $g_0, g_1, \dots, g_{n-1} \in \mathbb{F}_{q^m}$ are linearly independent over \mathbb{F}_q .

- $d = n - k + 1 \implies$ Gabidulin codes are MRD codes.

Reed–Solomon vs. Gabidulin Codes — BMD Decoding



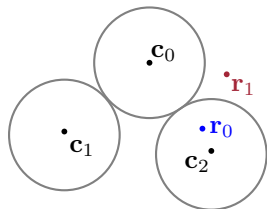
BMD decoding: $\tau = \lfloor \frac{d-1}{2} \rfloor$

→ decoding result: **unique** or **failure**

Algorithms	RS Codes	Gabidulin Codes
system of equations	Peterson, Gorenstein–Zierler	Roth, Gabidulin
Euclidean algorithm	Sugiyama <i>et al.</i> , Gao	Gabidulin
shift–register synth.	Berlekamp–Massey	Paramonov–Tretjakov, Richter–Plass–Sidorenko
interpolation	Welch–Berlekamp	Loidreau

Many parallels between RS and Gabidulin codes!

Reed–Solomon vs. Gabidulin Codes — BMD Decoding



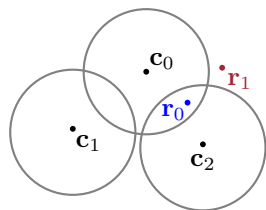
BMD decoding: $\tau = \lfloor \frac{d-1}{2} \rfloor$

→ decoding result: **unique** or **failure**

Algorithms	RS Codes	Gabidulin Codes
system of equations	Peterson, Gorenstein–Zierler	Roth, Gabidulin
Euclidean algorithm	Sugiyama <i>et al.</i> , Gao	Gabidulin
shift–register synth.	Berlekamp–Massey	Paramonov–Tretjakov, Richter–Plass–Sidorenko
interpolation	Welch–Berlekamp	Loidreau

Many parallels between RS and Gabidulin codes!

Reed–Solomon vs. Gabidulin Codes — List Decoding



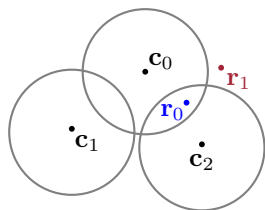
List decoding: $\tau > \lfloor \frac{d-1}{2} \rfloor$

→ decoding result: (empty) list

Algorithms	RS Codes	Gabidulin Codes
Interpolation-based	Sudan, Guruswami–Sudan (and many variants/ accelerations)	?

- Is polynomial-time list decoding possible for rank-metric codes?
- In particular for Gabidulin codes?

Reed–Solomon vs. Gabidulin Codes — List Decoding



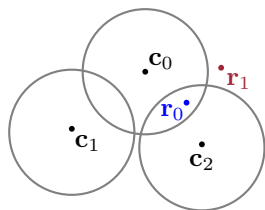
List decoding: $\tau > \lfloor \frac{d-1}{2} \rfloor$

→ decoding result: (empty) list

Algorithms	RS Codes	Gabidulin Codes
Interpolation-based	Sudan, Guruswami–Sudan (and many variants/ accelerations)	?

- Is polynomial-time list decoding possible for rank-metric codes?
- In particular for Gabidulin codes?

Reed–Solomon vs. Gabidulin Codes — List Decoding



List decoding: $\tau > \lfloor \frac{d-1}{2} \rfloor$

→ decoding result: (empty) list

Algorithms	RS Codes	Gabidulin Codes
Interpolation-based	Sudan, Guruswami–Sudan (and many variants/ accelerations)	?

- Is polynomial-time list decoding possible for rank-metric codes?
- In particular for Gabidulin codes?

Remark: List Decoding of Related Code Classes

- *Mahdavifar & Vardy* (2010): list decoding of **subcodes of lifted Gabidulin** codes ($\ell \leq \text{const.}$)
- *Guruswami, Narayanan & Wang* (2012): list decoding of lifted **folded** Gabidulin codes & **subcodes** thereof ($\ell \leq q^{m(s-1)}$ and $\ell \leq q^{s-1}$)
- *Mahdavifar & Vardy* (2012): list decoding of **folded** Gabidulin codes and of the corresponding lifting ($\ell \leq q^{m(s-1)}$)
- *Guruswami & Xing* (2013): list decoding of (other) **subcodes** of Gabidulin codes (rate does not tend to zero; $\ell \leq \mathcal{O}(1/\epsilon R)$)
- *Trautmann, Silberstein & Rosenthal* (2013): list decoding of **lifted Gabidulin codes** (using bilinear equations; complexity **exponential** in n)

- 1 Rank-Metric Codes & Decoding Principles
- 2 Problem Statement**
- 3 Bound on the List Size of Gabidulin Codes
 - Lower Bound
 - Asymptotic Behavior of Bounds
- 4 Bounds for Rank-Metric Codes
 - Interpretation as Constant-Rank Code
 - Upper Bound
 - Lower Bound
 - Asymptotic Behavior of Bounds
- 5 Conclusion & Outlook

Motivation & Problem Statement

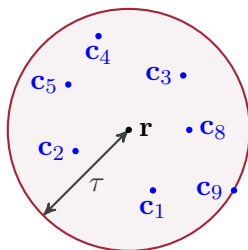
Motivation: Is **polynomial-time** list decoding possible?

Problem (Maximum List Size)

- $(n, M, d)_R$ code C over \mathbb{F}_{q^m}
- length $n \leq m$
- $\tau < d$

Find lower and upper bound on

$$\ell \stackrel{\text{def}}{=} \max_{\mathbf{r} \in \mathbb{F}_{q^m}^n} \left\{ |C \cap \mathcal{B}_\tau(\mathbf{r})| \right\}.$$



- lower exponential bound: **no** polynomial-time list decoding
- upper polynomial bound: **maybe** polynomial-time list decoding

Motivation & Problem Statement

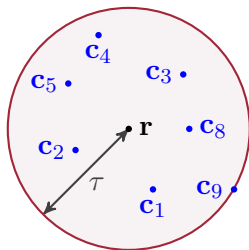
Motivation: Is **polynomial-time** list decoding possible?

Problem (Maximum List Size)

- $(n, M, d)_R$ code C over \mathbb{F}_{q^m}
- length $n \leq m$
- $\tau < d$

Find lower and upper bound on

$$\ell \stackrel{\text{def}}{=} \max_{\mathbf{r} \in \mathbb{F}_{q^m}^n} \left\{ |C \cap \mathcal{B}_\tau(\mathbf{r})| \right\}.$$



- lower exponential bound: **no** polynomial-time list decoding
- upper polynomial bound: **maybe** polynomial-time list decoding

- 1 Rank-Metric Codes & Decoding Principles
- 2 Problem Statement
- 3 Bound on the List Size of Gabidulin Codes**
 - Lower Bound
 - Asymptotic Behavior of Bounds
- 4 Bounds for Rank-Metric Codes
 - Interpretation as Constant-Rank Code
 - Upper Bound
 - Lower Bound
 - Asymptotic Behavior of Bounds
- 5 Conclusion & Outlook

Lower Bound for Gabidulin Codes

Theorem (Bound I: Lower Bound for Gabidulin Codes)

- $\text{Gab}[n, k]$ over \mathbb{F}_{q^m} with $n \leq m$ and $d = n - k + 1$
- $\tau < d$

Then, there exists a word $\mathbf{r} \in \mathbb{F}_{q^m}^n$ such that

$$\ell \geq |\text{Gab}[n, k] \cap \mathcal{B}_\tau(\mathbf{r})| \geq \frac{\binom{n}{n-\tau}}{(q^m)^{n-\tau-k}} \geq q^m q^{\tau(m+n)-\tau^2-md}$$

- For $n = m$: $\ell \geq q^{n(1-\epsilon)} \cdot q^{2n\tau-\tau^2-nd+n\epsilon}$
- exponential in n if $\tau \geq \underbrace{n - \sqrt{n(n-d+\epsilon)}}_{= \text{Johnson radius}}$ and $0 \leq \epsilon < 1$

Remark: for $n \leq m$ exp. if $\tau \geq \frac{m+n}{2} - \sqrt{\frac{(m+n)^2}{4} - m(d-\epsilon)}$

Theorem (Bound I: Lower Bound for Gabidulin Codes)

- $\text{Gab}[n, k]$ over \mathbb{F}_{q^m} with $n \leq m$ and $d = n - k + 1$
- $\tau < d$

Then, there exists a word $\mathbf{r} \in \mathbb{F}_{q^m}^n$ such that

$$\ell \geq |\text{Gab}[n, k] \cap \mathcal{B}_\tau(\mathbf{r})| \geq \frac{\binom{n}{n-\tau}}{(q^m)^{n-\tau-k}} \geq q^m q^{\tau(m+n)-\tau^2-md}$$

- For $n = m$: $\ell \geq q^{n(1-\epsilon)} \cdot q^{2n\tau-\tau^2-nd+n\epsilon}$
- exponential in n if $\tau \geq \underbrace{n - \sqrt{n(n-d+\epsilon)}}_{= \text{Johnson radius}}$ and $0 \leq \epsilon < 1$

Remark: for $n \leq m$ exp. if $\tau \geq \frac{m+n}{2} - \sqrt{\frac{(m+n)^2}{4} - m(d-\epsilon)}$

Lower Bound for Gabidulin Codes – Sketch of Proof

Sketch of proof: (Similar to *Justesen & Høholdt* and *Ben-Sasson, Kopparty & Radhakrishnan* for RS codes)

- $\mathcal{Q} \stackrel{\text{def}}{=} \text{set of all monic linearized polynomials of } \deg_q = n - \tau \text{ and root space over } \mathbb{F}_{q^n} \text{ of dimension } n - \tau \implies |\mathcal{Q}| = \binom{n}{n-\tau}$
- $\mathcal{P} \subset \mathcal{Q}$, s.t. all q -monomials of $\deg_q \geq k$ have same coefficients
- pigeonhole principle: There exist coefficients s.t. $|\mathcal{P}| \geq \frac{\binom{n}{n-\tau}}{\binom{q^m}{n-\tau-k}} \implies \text{For all } f(x), g(x) \in \mathcal{P} \implies \deg_q(f(x) - g(x)) < k$
- let \mathbf{r} be the evaluation of $f(x)$ at a basis of \mathbb{F}_{q^n} over \mathbb{F}_q
- let \mathbf{c} be the evaluation of $f(x) - g(x)$ at this basis
 $\implies \mathbf{r} - \mathbf{c}$ is the evaluation of $f(x) - f(x) + g(x) = g(x) \in \mathcal{P}$
 $\implies \dim \ker(\mathbf{r} - \mathbf{c}) = n - \tau \iff \text{rk}(\mathbf{r} - \mathbf{c}) = \tau$

Therefore, for **any** $g(x) \in \mathcal{P}$, the evaluation of $f(x) - g(x)$ is a codeword from $\text{Gab}[n, k]$, which has rank distance τ from \mathbf{r} .

$$\implies \ell \geq |\mathcal{P}|$$



Lower Bound for Gabidulin Codes – Sketch of Proof

Sketch of proof: (Similar to *Justesen & Høholdt* and *Ben-Sasson, Kopparty & Radhakrishnan* for RS codes)

- $\mathcal{Q} \stackrel{\text{def}}{=} \text{set of all monic linearized polynomials of } \deg_q = n - \tau \text{ and root space over } \mathbb{F}_{q^n} \text{ of dimension } n - \tau \implies |\mathcal{Q}| = \binom{n}{n-\tau}$
- $\mathcal{P} \subset \mathcal{Q}$, s.t. all q -monomials of $\deg_q \geq k$ have same coefficients
- pigeonhole principle: There exist coefficients s.t. $|\mathcal{P}| \geq \frac{\binom{n}{n-\tau}}{(q^m)^{n-\tau-k}} \implies \text{For all } f(x), g(x) \in \mathcal{P} \implies \deg_q(f(x) - g(x)) < k$
- let \mathbf{r} be the evaluation of $f(x)$ at a basis of \mathbb{F}_{q^n} over \mathbb{F}_q
- let \mathbf{c} be the evaluation of $f(x) - g(x)$ at this basis
 $\implies \mathbf{r} - \mathbf{c}$ is the evaluation of $f(x) - f(x) + g(x) = g(x) \in \mathcal{P}$
 $\implies \dim \ker(\mathbf{r} - \mathbf{c}) = n - \tau \iff \text{rk}(\mathbf{r} - \mathbf{c}) = \tau$

Therefore, for **any** $g(x) \in \mathcal{P}$, the evaluation of $f(x) - g(x)$ is a codeword from $\text{Gab}[n, k]$, which has rank distance τ from \mathbf{r} .

$$\implies \ell \geq |\mathcal{P}|$$



Lower Bound for Gabidulin Codes – Sketch of Proof

Sketch of proof: (Similar to *Justesen & Høholdt* and *Ben-Sasson, Kopparty & Radhakrishnan* for RS codes)

- $\mathcal{Q} \stackrel{\text{def}}{=} \text{set of all monic linearized polynomials of } \deg_q = n - \tau \text{ and root space over } \mathbb{F}_{q^n} \text{ of dimension } n - \tau \implies |\mathcal{Q}| = \binom{n}{n-\tau}$
- $\mathcal{P} \subset \mathcal{Q}$, s.t. all q -monomials of $\deg_q \geq k$ have same coefficients
- pigeonhole principle: There exist coefficients s.t. $|\mathcal{P}| \geq \frac{\binom{n}{n-\tau}}{(q^m)^{n-\tau-k}}$
 $\implies \text{For all } f(x), g(x) \in \mathcal{P} \implies \deg_q(f(x) - g(x)) < k$
- let \mathbf{r} be the evaluation of $f(x)$ at a basis of \mathbb{F}_{q^n} over \mathbb{F}_q
- let \mathbf{c} be the evaluation of $f(x) - g(x)$ at this basis
 $\implies \mathbf{r} - \mathbf{c}$ is the evaluation of $f(x) - f(x) + g(x) = g(x) \in \mathcal{P}$
 $\implies \dim \ker(\mathbf{r} - \mathbf{c}) = n - \tau \iff \text{rk}(\mathbf{r} - \mathbf{c}) = \tau$

Therefore, for **any** $g(x) \in \mathcal{P}$, the evaluation of $f(x) - g(x)$ is a codeword from $\text{Gab}[n, k]$, which has rank distance τ from \mathbf{r} .

$$\implies \ell \geq |\mathcal{P}|$$



Lower Bound for Gabidulin Codes – Sketch of Proof

Sketch of proof: (Similar to *Justesen & Høholdt* and *Ben-Sasson, Kopparty & Radhakrishnan* for RS codes)

- $\mathcal{Q} \stackrel{\text{def}}{=} \text{set of all monic linearized polynomials of } \deg_q = n - \tau \text{ and root space over } \mathbb{F}_{q^n} \text{ of dimension } n - \tau \implies |\mathcal{Q}| = \binom{n}{n-\tau}$
- $\mathcal{P} \subset \mathcal{Q}$, s.t. all q -monomials of $\deg_q \geq k$ have same coefficients
- pigeonhole principle: There exist coefficients s.t. $|\mathcal{P}| \geq \frac{\binom{n}{n-\tau}}{(q^m)^{n-\tau-k}}$
 $\implies \text{For all } f(x), g(x) \in \mathcal{P} \implies \deg_q(f(x) - g(x)) < k$
- let \mathbf{r} be the evaluation of $f(x)$ at a basis of \mathbb{F}_{q^n} over \mathbb{F}_q
- let \mathbf{c} be the evaluation of $f(x) - g(x)$ at this basis
 $\implies \mathbf{r} - \mathbf{c}$ is the evaluation of $f(x) - f(x) + g(x) = g(x) \in \mathcal{P}$
 $\implies \dim \ker(\mathbf{r} - \mathbf{c}) = n - \tau \iff \text{rk}(\mathbf{r} - \mathbf{c}) = \tau$

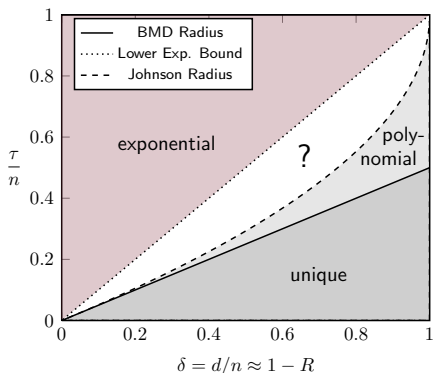
Therefore, for **any** $g(x) \in \mathcal{P}$, the evaluation of $f(x) - g(x)$ is a codeword from $\text{Gab}[n, k]$, which has rank distance τ from \mathbf{r} .

$$\implies \ell \geq |\mathcal{P}|$$

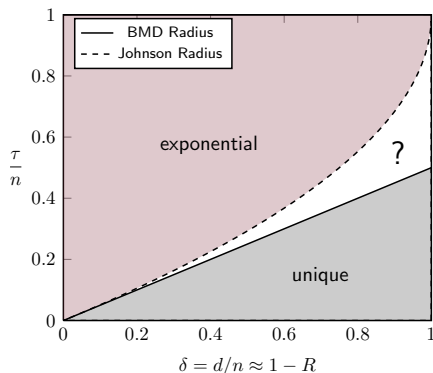


Asymptotic Behavior of Bounds on the List Size

Reed–Solomon codes



Gabidulin codes

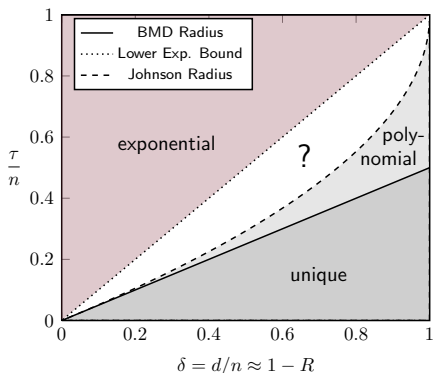


- different behavior?
- connect unknown regions?

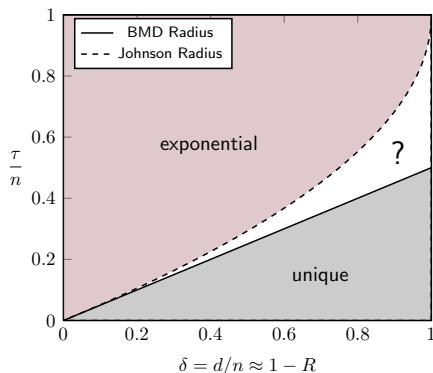
Remark: Rudra & Wootters (Oct. 2013): many RS codes are list decodable beyond the Johnson radius (?)

Asymptotic Behavior of Bounds on the List Size

Reed–Solomon codes



Gabidulin codes



- different behavior?
- connect unknown regions?

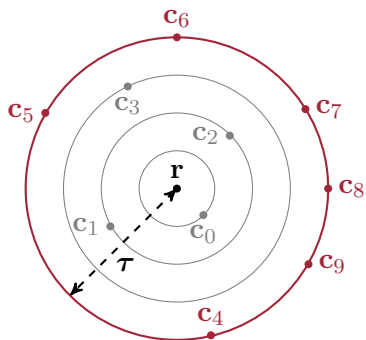
Remark: Rudra & Wootters (Oct. 2013): many RS codes are list decodable beyond the Johnson radius (?)

- 1 Rank-Metric Codes & Decoding Principles
- 2 Problem Statement
- 3 Bound on the List Size of Gabidulin Codes
 - Lower Bound
 - Asymptotic Behavior of Bounds
- 4 Bounds for Rank-Metric Codes**
 - Interpretation as Constant-Rank Code
 - Upper Bound
 - Lower Bound
 - Asymptotic Behavior of Bounds
- 5 Conclusion & Outlook

Interpretation as Constant-Rank Code

decoding list:

$$\mathcal{L} = \{\mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_{\ell-1}\} = \mathcal{C} \cap \mathcal{B}_\tau(\mathbf{r}) = \sum_{i=0}^{\tau} (\mathcal{C} \cap \mathcal{S}_i(\mathbf{r}))$$



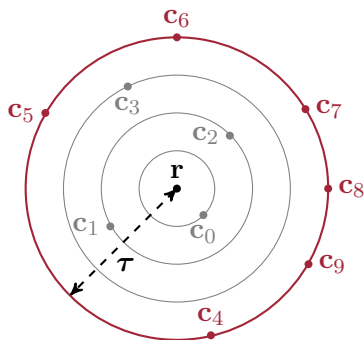
- Consider codewords $\mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_{\ell-1}$ in distance *exactly* τ
- Define $\bar{\mathcal{L}} = \{\mathbf{r} - \mathbf{c}_0, \dots, \mathbf{r} - \mathbf{c}_{\ell-1}\}$
- $\text{rk}(\mathbf{r} - \mathbf{c}_i - (\mathbf{r} - \mathbf{c}_j)) = \text{rk}(\mathbf{c}_j - \mathbf{c}_i) \geq d$
 $\implies \bar{\mathcal{L}}$ is a **constant-rank code** of rank τ and min. distance $\geq d$
- $|\mathcal{C} \cap \mathcal{S}_\tau(\mathbf{r})| \leq A_{q^m}^R(n, d_R \geq d, \tau)$

\implies Bounds on the cardinality of constant-rank codes can be used for bounding the list size

Interpretation as Constant-Rank Code

decoding list:

$$\mathcal{L} = \{\mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_{\ell-1}\} = \mathcal{C} \cap \mathcal{B}_\tau(\mathbf{r}) = \sum_{i=0}^{\tau} (\mathcal{C} \cap \mathcal{S}_i(\mathbf{r}))$$



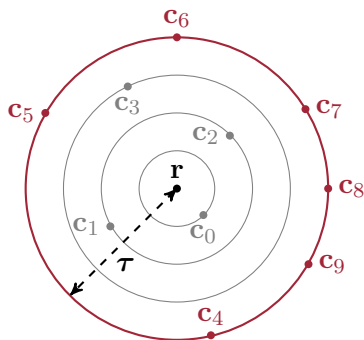
- Consider codewords $\mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_{\ell-1}$ in distance *exactly* τ
- Define $\bar{\mathcal{L}} = \{\mathbf{r} - \mathbf{c}_0, \dots, \mathbf{r} - \mathbf{c}_{\ell-1}\}$
- $\text{rk}(\mathbf{r} - \mathbf{c}_i - (\mathbf{r} - \mathbf{c}_j)) = \text{rk}(\mathbf{c}_j - \mathbf{c}_i) \geq d$
 $\implies \bar{\mathcal{L}}$ is a **constant-rank code** of rank τ and min. distance $\geq d$
- $|\mathcal{C} \cap \mathcal{S}_\tau(\mathbf{r})| \leq A_{q^m}^R(n, d_R \geq d, \tau)$

\implies Bounds on the cardinality of constant-rank codes can be used for bounding the list size

Interpretation as Constant-Rank Code

decoding list:

$$\mathcal{L} = \{\mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_{\ell-1}\} = \mathcal{C} \cap \mathcal{B}_\tau(\mathbf{r}) = \sum_{i=0}^{\tau} (\mathcal{C} \cap \mathcal{S}_i(\mathbf{r}))$$



- Consider codewords $\mathbf{c}_0, \mathbf{c}_1, \dots, \mathbf{c}_{\ell-1}$ in distance *exactly* τ
- Define $\bar{\mathcal{L}} = \{\mathbf{r} - \mathbf{c}_0, \dots, \mathbf{r} - \mathbf{c}_{\ell-1}\}$
- $\text{rk}(\mathbf{r} - \mathbf{c}_i - (\mathbf{r} - \mathbf{c}_j)) = \text{rk}(\mathbf{c}_j - \mathbf{c}_i) \geq d$
 $\implies \bar{\mathcal{L}}$ is a **constant-rank code** of rank τ and min. distance $\geq d$
- $|\mathcal{C} \cap \mathcal{S}_\tau(\mathbf{r})| \leq A_{q^m}^R(n, d_R \geq d, \tau)$

\implies Bounds on the cardinality of constant-rank codes can be used for bounding the list size

An Upper Bound on the List Size

Theorem (Bound II: Upper Bound for any Rank-Metric Code)

Let $\lfloor (d-1)/2 \rfloor \leq \tau < d \leq n \leq m$. Then, for **any** $(n, M, d)_R$ code C :

$$\begin{aligned} \ell &= \max_{\mathbf{r} \in \mathbb{F}_q^{n \times m}} \left\{ |C \cap \mathcal{B}_\tau(\mathbf{r})| \right\} \leq 1 + \sum_{t=\lfloor \frac{d-1}{2} \rfloor + 1}^{\tau} \frac{\binom{n}{2t+1-d}}{\binom{t}{2t+1-d}} \\ &\leq 1 + 4 \cdot \left(\tau - \lfloor \frac{d-1}{2} \rfloor \right) \cdot q^{(2\tau-d+1)(n-\lfloor (d-1)/2 \rfloor - 1)} \end{aligned}$$

- Exponential in $n \leq m$ for any $\tau > \lfloor (d-1)/2 \rfloor$
- Does not provide any conclusion if polynomial-time list decoding is possible or not...

An Upper Bound on the List Size

Theorem (Bound II: Upper Bound for any Rank-Metric Code)

Let $\lfloor (d-1)/2 \rfloor \leq \tau < d \leq n \leq m$. Then, for **any** $(n, M, d)_R$ code C :

$$\begin{aligned} \ell &= \max_{\mathbf{r} \in \mathbb{F}_q^{n \times m}} \left\{ |C \cap \mathcal{B}_\tau(\mathbf{r})| \right\} \leq 1 + \sum_{t=\lfloor \frac{d-1}{2} \rfloor + 1}^{\tau} \frac{\binom{n}{2t+1-d}}{\binom{t}{2t+1-d}} \\ &\leq 1 + 4 \cdot \left(\tau - \lfloor \frac{d-1}{2} \rfloor \right) \cdot q^{(2\tau-d+1)(n-\lfloor (d-1)/2 \rfloor - 1)} \end{aligned}$$

- Exponential in $n \leq m$ for any $\tau > \lfloor (d-1)/2 \rfloor$
- Does not provide any conclusion if polynomial-time list decoding is possible or not...

Upper Bound for Rank Metric Codes – Sketch of Proof

Sketch of Proof:

- $\mathbf{C} \cap \mathcal{S}_t(\mathbf{r}) = \{\mathbf{r} - \mathbf{c}_1, \dots, \mathbf{r} - \mathbf{c}_{\bar{\ell}}\}$
 \implies this is an $(n, M, d_R \geq d, t)_{q^m}$ **constant-rank code**
- Use max. cardinality of such a constant-rank code as upper bound:
 $|\mathbf{C} \cap \mathcal{S}_t(\mathbf{r})| \leq A_{q^m}^R(n, d_R \geq d, t) \leq A_{q^m}^R(n, d, t)$
- Use connection between constant-rank and constant-dimension codes from *Gadouleau & Yan (2010)*:
 $A_{q^m}^R(n, d, t) \leq A_q^S(n, d_S = 2(d - t), t)$
- Use upper bound on cardinality of constant-dimension codes by *Wang, Xing, Safavi-Naini (2003)*:
 $A_q^S(n, d_S = 2(d - t), t) \leq \frac{\binom{n}{t - (d - t) + 1}}{\binom{t}{t - (d - t) + 1}}$

Summing up for $t = \lfloor (d-1)/2 \rfloor + 1, \dots, \tau$ gives the statement. \square

Upper Bound for Rank Metric Codes – Sketch of Proof

Sketch of Proof:

- $\mathcal{C} \cap \mathcal{S}_t(\mathbf{r}) = \{\mathbf{r} - \mathbf{c}_1, \dots, \mathbf{r} - \mathbf{c}_{\bar{\ell}}\}$
 \implies this is an $(n, M, d_R \geq d, t)_{q^m}$ **constant-rank code**
- Use max. cardinality of such a constant-rank code as upper bound:
 $|\mathcal{C} \cap \mathcal{S}_t(\mathbf{r})| \leq A_{q^m}^R(n, d_R \geq d, t) \leq A_{q^m}^R(n, d, t)$
- Use connection between constant-rank and **constant-dimension codes** from *Gadouleau & Yan (2010)*:
 $A_{q^m}^R(n, d, t) \leq A_q^S(n, d_S = 2(d - t), t)$
- Use upper bound on cardinality of constant-dimension codes by *Wang, Xing, Safavi-Naini (2003)*:
 $A_q^S(n, d_S = 2(d - t), t) \leq \frac{\binom{n}{t - (d - t) + 1}}{\binom{t}{t - (d - t) + 1}}$

Summing up for $t = \lfloor (d-1)/2 \rfloor + 1, \dots, \tau$ gives the statement. □

Upper Bound for Rank Metric Codes – Sketch of Proof

Sketch of Proof:

- $C \cap \mathcal{S}_t(\mathbf{r}) = \{\mathbf{r} - \mathbf{c}_1, \dots, \mathbf{r} - \mathbf{c}_{\bar{\ell}}\}$
 \implies this is an $(n, M, d_R \geq d, t)_{q^m}$ **constant-rank code**
- Use max. cardinality of such a constant-rank code as upper bound:
 $|C \cap \mathcal{S}_t(\mathbf{r})| \leq A_{q^m}^R(n, d_R \geq d, t) \leq A_{q^m}^R(n, d, t)$
- Use connection between constant-rank and **constant-dimension codes** from *Gadouleau & Yan (2010)*:
 $A_{q^m}^R(n, d, t) \leq A_q^S(n, d_S = 2(d - t), t)$
- Use upper bound on cardinality of constant-dimension codes by *Wang, Xing, Safavi-Naini (2003)*:
 $A_q^S(n, d_S = 2(d - t), t) \leq \frac{\binom{n}{t - (d - t) + 1}}{\binom{t}{t - (d - t) + 1}}$

Summing up for $t = \lfloor (d-1)/2 \rfloor + 1, \dots, \tau$ gives the statement. □

Upper Bound for Rank Metric Codes – Sketch of Proof

Sketch of Proof:

- $\mathcal{C} \cap \mathcal{S}_t(\mathbf{r}) = \{\mathbf{r} - \mathbf{c}_1, \dots, \mathbf{r} - \mathbf{c}_{\bar{\ell}}\}$
 \implies this is an $(n, M, d_R \geq d, t)_{q^m}$ **constant-rank code**
- Use max. cardinality of such a constant-rank code as upper bound:
 $|\mathcal{C} \cap \mathcal{S}_t(\mathbf{r})| \leq A_{q^m}^R(n, d_R \geq d, t) \leq A_{q^m}^R(n, d, t)$
- Use connection between constant-rank and **constant-dimension codes** from *Gadouleau & Yan (2010)*:
 $A_{q^m}^R(n, d, t) \leq A_q^S(n, d_S = 2(d - t), t)$
- Use upper bound on cardinality of constant-dimension codes by *Wang, Xing, Safavi-Naini (2003)*:
 $A_q^S(n, d_S = 2(d - t), t) \leq \frac{\binom{n}{t - (d - t) + 1}}{\binom{t}{t - (d - t) + 1}}$

Summing up for $t = \lfloor (d-1)/2 \rfloor + 1, \dots, \tau$ gives the statement. □

A Lower Bound on the List Size

Theorem (Bound III: Lower Bound for some Rank-Metric Code)

Let $\lfloor (d-1)/2 \rfloor \leq \tau < d \leq n \leq m$ and $\tau \leq n - \tau$.

Then, there exists an $(n, M, d_R \geq d)_R$ code \mathbf{C} over \mathbb{F}_{q^m} and a word $\mathbf{r} \in \mathbb{F}_{q^m}^n$ such that

$$\ell = \ell(m, n, d, \tau) \geq |\mathbf{C} \cap \mathcal{B}_\tau(\mathbf{r})| \geq q^{(n-\tau)(\tau - \lfloor (d-1)/2 \rfloor)}.$$

- There exists a rank-metric code such that max. list size is **exponential** in n for $\tau > \lfloor (d-1)/2 \rfloor$.
 \implies no polynomial-time list decoding for these codes
- \mathbf{C} might be non-linear and non-MRD
- $\tau \leq n - \tau$ is fulfilled for $\tau = \lfloor (d-1)/2 \rfloor + 1$ and $k > 1$

A Lower Bound on the List Size

Theorem (Bound III: Lower Bound for some Rank-Metric Code)

Let $\lfloor (d-1)/2 \rfloor \leq \tau < d \leq n \leq m$ and $\tau \leq n - \tau$.

Then, there exists an $(n, M, d_R \geq d)_R$ code C over \mathbb{F}_{q^m} and a word $\mathbf{r} \in \mathbb{F}_{q^m}^n$ such that

$$\ell = \ell(m, n, d, \tau) \geq |C \cap \mathcal{B}_\tau(\mathbf{r})| \geq q^{(n-\tau)(\tau - \lfloor (d-1)/2 \rfloor)}.$$

- There exists a rank-metric code such that max. list size is **exponential** in n for $\tau > \lfloor (d-1)/2 \rfloor$.
 \implies no polynomial-time list decoding for these codes
- C might be non-linear and non-MRD
- $\tau \leq n - \tau$ is fulfilled for $\tau = \lfloor (d-1)/2 \rfloor + 1$ and $k > 1$

A Lower Bound on the List Size

Theorem (Bound III: Lower Bound for some Rank-Metric Code)

Let $\lfloor (d-1)/2 \rfloor \leq \tau < d \leq n \leq m$ and $\tau \leq n - \tau$.

Then, there exists an $(n, M, d_R \geq d)_R$ code C over \mathbb{F}_{q^m} and a word $\mathbf{r} \in \mathbb{F}_{q^m}^n$ such that

$$\ell = \ell(m, n, d, \tau) \geq |C \cap \mathcal{B}_\tau(\mathbf{r})| \geq q^{(n-\tau)(\tau - \lfloor (d-1)/2 \rfloor)}.$$

- There exists a rank-metric code such that max. list size is **exponential** in n for $\tau > \lfloor (d-1)/2 \rfloor$.
 \implies no polynomial-time list decoding for these codes
- C might be non-linear and non-MRD
- $\tau \leq n - \tau$ is fulfilled for $\tau = \lfloor (d-1)/2 \rfloor + 1$ and $k > 1$

Lower Bound for Rank Metric Codes — Sketch of Proof

Sketch of Proof:

- Use two constant-dimension codes (lifted MRD codes) to construct (similar to *Gadouleau & Yan*)
 - an $(n, M, d_R \geq d, \tau)_{q^m}$ **constant-rank code**
 - with cardinality $q^{(n-\tau)(\tau - \lfloor (d-1)/2 \rfloor)}$

Denote the codewords of this constant-rank code by $\{\mathbf{a}_0, \mathbf{a}_1, \dots\}$.

- Choose $\mathbf{r} = \mathbf{0}$:
 - $\text{rk}(\mathbf{r} - \mathbf{a}_i) = \text{rk}(\mathbf{a}_i) = \tau$ for all i (constant-rank code)
 - $d_R(\mathbf{a}_i, \mathbf{a}_j) = \text{rk}(\mathbf{a}_i - \mathbf{a}_j) \geq d$
- $\Rightarrow \mathbf{a}_0, \mathbf{a}_1, \dots$ are codewords of a code with rank distance at least d
- \Rightarrow and lie all on a sphere of radius τ around \mathbf{r}

There exists an $(n, M, d_R \geq d)_R$ code C of min. rank distance at least d s.t. $\ell \geq |C \cap \mathcal{S}_\tau(\mathbf{r})| = |CR| = q^{(n-\tau)(\tau - \lfloor (d-1)/2 \rfloor)}$. \square

Lower Bound for Rank Metric Codes — Sketch of Proof

Sketch of Proof:

- Use two constant-dimension codes (lifted MRD codes) to construct (similar to *Gadouleau & Yan*)
 - an $(n, M, d_R \geq d, \tau)_{q^m}$ **constant-rank code**
 - with cardinality $q^{(n-\tau)(\tau - \lfloor (d-1)/2 \rfloor)}$

Denote the codewords of this constant-rank code by $\{\mathbf{a}_0, \mathbf{a}_1, \dots\}$.

- Choose $\mathbf{r} = \mathbf{0}$:
 - $\text{rk}(\mathbf{r} - \mathbf{a}_i) = \text{rk}(\mathbf{a}_i) = \tau$ for all i (constant-rank code)
 - $d_R(\mathbf{a}_i, \mathbf{a}_j) = \text{rk}(\mathbf{a}_i - \mathbf{a}_j) \geq d$

$\Rightarrow \mathbf{a}_0, \mathbf{a}_1, \dots$ are codewords of a code with rank distance at least d

\Rightarrow and lie all on a sphere of radius τ around \mathbf{r}

There exists an $(n, M, d_R \geq d)_R$ code C of min. rank distance at least d s.t. $\ell \geq |C \cap \mathcal{S}_\tau(\mathbf{r})| = |CR| = q^{(n-\tau)(\tau - \lfloor (d-1)/2 \rfloor)}$. \square

Lower Bound for Rank Metric Codes — Sketch of Proof

Sketch of Proof:

- Use two constant-dimension codes (lifted MRD codes) to construct (similar to *Gadouleau & Yan*)
 - an $(n, M, d_R \geq d, \tau)_{q^m}$ **constant-rank code**
 - with cardinality $q^{(n-\tau)(\tau - \lfloor (d-1)/2 \rfloor)}$

Denote the codewords of this constant-rank code by $\{\mathbf{a}_0, \mathbf{a}_1, \dots\}$.

- Choose $\mathbf{r} = \mathbf{0}$:
 - $\text{rk}(\mathbf{r} - \mathbf{a}_i) = \text{rk}(\mathbf{a}_i) = \tau$ for all i (constant-rank code)
 - $d_R(\mathbf{a}_i, \mathbf{a}_j) = \text{rk}(\mathbf{a}_i - \mathbf{a}_j) \geq d$
- $\Rightarrow \mathbf{a}_0, \mathbf{a}_1, \dots$ are codewords of a code with **rank distance at least d**
 \Rightarrow and lie all on a sphere of **radius τ around \mathbf{r}**

There exists an $(n, M, d_R \geq d)_R$ code C of min. rank distance at least d s.t. $\ell \geq |C \cap \mathcal{S}_\tau(\mathbf{r})| = |CR| = q^{(n-\tau)(\tau - \lfloor (d-1)/2 \rfloor)}$. \square

Lower Bound for Rank Metric Codes — Sketch of Proof

Sketch of Proof:

- Use two constant-dimension codes (lifted MRD codes) to construct (similar to *Gadouleau & Yan*)
 - an $(n, M, d_R \geq d, \tau)_{q^m}$ **constant-rank code**
 - with cardinality $q^{(n-\tau)(\tau - \lfloor (d-1)/2 \rfloor)}$

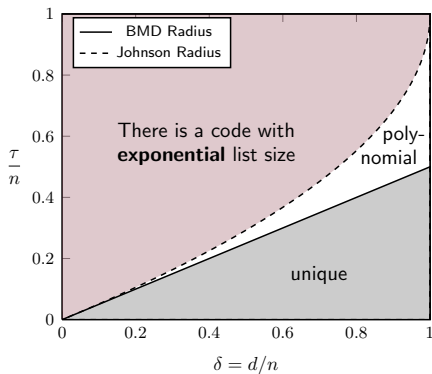
Denote the codewords of this constant-rank code by $\{\mathbf{a}_0, \mathbf{a}_1, \dots\}$.

- Choose $\mathbf{r} = \mathbf{0}$:
 - $\text{rk}(\mathbf{r} - \mathbf{a}_i) = \text{rk}(\mathbf{a}_i) = \tau$ for all i (constant-rank code)
 - $d_R(\mathbf{a}_i, \mathbf{a}_j) = \text{rk}(\mathbf{a}_i - \mathbf{a}_j) \geq d$
- $\Rightarrow \mathbf{a}_0, \mathbf{a}_1, \dots$ are codewords of a code with **rank distance at least d**
 \Rightarrow and lie all on a sphere of **radius τ around \mathbf{r}**

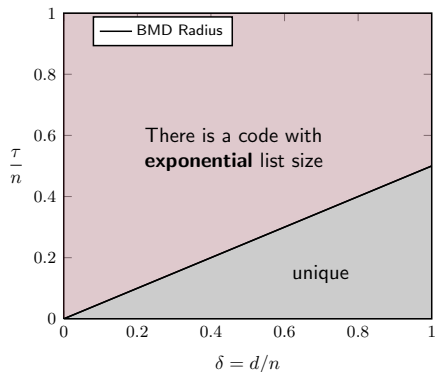
There exists an $(n, M, d_R \geq d)_R$ code C of min. rank distance at least d
s.t. $\ell \geq |C \cap \mathcal{S}_\tau(\mathbf{r})| = |CR| = q^{(n-\tau)(\tau - \lfloor (d-1)/2 \rfloor)}$. \square

Asymptotic Behavior of Bounds on the List Size

codes in Hamming metric



codes in rank metric



- different behavior
- no polynomial Johnson-like upper bound in rank metric (depending only on n and d)!

Tighter Lower Bound for Special Cases

Lemma (Lower Bound for $\tau = d/2$ or large m)

Let $\lfloor (d-1)/2 \rfloor < \tau < d < n$ and $\tau \leq n - \tau$.

If

- $\tau = d/2$ or
- $m \geq (n - \tau)(2\tau - d + 1) + \tau + 1$,

there exists an $(n, M, d_R = d)_R$ code \mathbf{C} over \mathbb{F}_{q^m} and a word $\mathbf{r} \in \mathbb{F}_{q^m}^n$ such that

$$\ell = \ell(m, n, d, \tau) \geq |\mathbf{C} \cap \mathcal{B}_\tau(\mathbf{r})| \geq q^{(n-\tau)(2\tau-d+1)}.$$

\implies This lower bound is asymptotically tight!

- 1 Rank-Metric Codes & Decoding Principles
- 2 Problem Statement
- 3 Bound on the List Size of Gabidulin Codes
 - Lower Bound
 - Asymptotic Behavior of Bounds
- 4 Bounds for Rank-Metric Codes
 - Interpretation as Constant-Rank Code
 - Upper Bound
 - Lower Bound
 - Asymptotic Behavior of Bounds
- 5 Conclusion & Outlook

Conclusion & Outlook

Lower bound for **Gabidulin codes**:

- no polynomial-time list decoding for $\tau \geq n - \sqrt{n(n-d+\epsilon)}$
- **open question**: Behavior up to this radius?
- **open question**: Relation between RS and Gabidulin codes?

Upper bound for **any** rank-metric code:

- exponential in n for $\tau > \lfloor (d-1)/2 \rfloor$
- **open question**: Code classes with polynomial upper bound?

Lower bound for rank-metric codes:

- there exists a rank-metric code with exponential list size for any $\tau > \lfloor (d-1)/2 \rfloor$
- there is no polynomial Johnson-like upper bound
- **open question**: Are there such **linear** rank-metric codes?

Conclusion & Outlook

Lower bound for **Gabidulin codes**:

- no polynomial-time list decoding for $\tau \geq n - \sqrt{n(n-d+\epsilon)}$
- **open question**: Behavior up to this radius?
- **open question**: Relation between RS and Gabidulin codes?

Upper bound for **any** rank-metric code:

- exponential in n for $\tau > \lfloor (d-1)/2 \rfloor$
- **open question**: Code classes with polynomial upper bound?

Lower bound for rank-metric codes:

- there exists a rank-metric code with exponential list size for any $\tau > \lfloor (d-1)/2 \rfloor$
- there is no polynomial Johnson-like upper bound
- **open question**: Are there such **linear** rank-metric codes?

Conclusion & Outlook

Lower bound for **Gabidulin codes**:

- no polynomial-time list decoding for $\tau \geq n - \sqrt{n(n-d+\epsilon)}$
- **open question**: Behavior up to this radius?
- **open question**: Relation between RS and Gabidulin codes?

Upper bound for **any** rank-metric code:

- exponential in n for $\tau > \lfloor (d-1)/2 \rfloor$
- **open question**: Code classes with polynomial upper bound?

Lower bound for rank-metric codes:

- there exists a rank-metric code with exponential list size for any $\tau > \lfloor (d-1)/2 \rfloor$
- there is no polynomial Johnson-like upper bound
- **open question**: Are there such **linear** rank-metric codes?

Thank you...

...for your attention!

תודה!