Bounds on List Decoding of Rank-Metric Codes

Antonia Wachter-Zeh

Institute of Communications Engineering, Ulm University &
Institut de Recherche Mathématique de Rennes, Université de Rennes 1

September 18, 2013
Non-Coherent Random Linear Network Coding

- internal structure unknown
- packets: vectors over finite field
- nodes: random linear combinations

→ higher throughput than routing!

BUT: high error propagation

Silva, Kschischang & Kötter (2008): Error control using lifted Gabidulin codes
Non-Coherent Random Linear Network Coding

- internal structure unknown
- packets: vectors over finite field
- nodes: random linear combinations

⇒ higher throughput than routing!
BUT: high error propagation

Silva, Kschischang & Kötter (2008):
Error control using lifted Gabidulin codes
Outline

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

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

Rank Metric

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

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

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

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

- \(f(x) \overset{\text{def}}{=} \sum_{i=0}^{d_f} f_i x^{[i]} = \sum_{i=0}^{d_f} f_i x^{q^i} \) \(\) with \(f_i \in \mathbb{F}_{q^m}\)
- \(q\)-degree: \(\text{deg}_q f(x) = d_f\)
## Rank-Metric Codes

### Rank Metric

- **Bijective map** \( x \in \mathbb{F}_{q^m}^n \mapsto X \in \mathbb{F}_q^{m \times n} \)
- **Rank norm**: \( \text{rk}(x) \overset{\text{def}}{=} \text{rank of } X \text{ over } \mathbb{F}_q \)

### Minimum Rank Distance

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

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

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

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


**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

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

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

$d = n - k + 1 \implies$ Gabidulin codes are MRD codes.
BMD decoding: \[ \tau = \left\lfloor \frac{d-1}{2} \right\rfloor \]

\( \rightarrow \) decoding result: unique or failure

Many parallels between RS and Gabidulin codes!
Reed–Solomon vs. Gabidulin Codes — BMD Decoding

BMD decoding: \( \tau = \left\lfloor \frac{d-1}{2} \right\rfloor \)

\( \rightarrow \) decoding result: unique or failure

<table>
<thead>
<tr>
<th>Algorithms</th>
<th>RS Codes</th>
<th>Gabidulin Codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>system of equations</td>
<td>Peterson, Gorenstein–Zierler</td>
<td>Roth, Gabidulin</td>
</tr>
<tr>
<td>Euclidean algorithm</td>
<td>Sugiyama et al., Gao</td>
<td>Gabidulin</td>
</tr>
<tr>
<td>interpolation</td>
<td>Welch–Berlekamp</td>
<td>Loidreau</td>
</tr>
</tbody>
</table>

Many parallels between RS and Gabidulin codes!
Reed–Solomon vs. Gabidulin Codes — List Decoding

List decoding: $\tau \geq \left\lfloor \frac{d-1}{2} \right\rfloor$

→ decoding result: list or failure

<table>
<thead>
<tr>
<th>Algorithms</th>
<th>RS Codes</th>
<th>Gabidulin Codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interpolation-based</td>
<td>Sudan, Guruswami–Sudan</td>
<td>?</td>
</tr>
<tr>
<td></td>
<td>(and many variants/accelerations)</td>
<td></td>
</tr>
</tbody>
</table>

- Is polynomial-time list decoding possible for rank-metric codes?
- In particular for Gabidulin codes?
List decoding: \( \tau \geq \left\lfloor \frac{d-1}{2} \right\rfloor \)

\( \rightarrow \) decoding result: list or failure

<table>
<thead>
<tr>
<th>Algorithms</th>
<th>RS Codes</th>
<th>Gabidulin Codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interpolation-based</td>
<td>Sudan, Guruswami–Sudan (and many variants/accelerations)</td>
<td>?</td>
</tr>
</tbody>
</table>

- Is polynomial-time list decoding possible for rank-metric codes?
- In particular for Gabidulin codes?
List decoding: \[ \tau \geq \left\lfloor \frac{d-1}{2} \right\rfloor \]
\[ \rightarrow \text{decoding result: list or failure} \]

<table>
<thead>
<tr>
<th>Algorithms</th>
<th>RS Codes</th>
<th>Gabidulin Codes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interpolation-based</td>
<td>Sudan, Guruswami–Sudan</td>
<td>?</td>
</tr>
<tr>
<td></td>
<td>(and many variants/accelerations)</td>
<td></td>
</tr>
</tbody>
</table>

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

1. Rank-Metric Codes & Decoding Principles
2. Problem Statement
3. A Bound on the List Size of Gabidulin Codes
   - Lower Bound
   - Asymptotic Behavior of Bounds
4. Bounds for General Rank-Metric Codes
   - Interpretation as Constant-Rank Code
   - Upper Bound
   - Lower Bound
   - Asymptotic Behavior of Bounds
5. Conclusion & Outlook
Motivation: Is polynomial-time list decoding possible?

Problem (Maximum List Size)

\((n, M, d)\) code \(C\) over \(\mathbb{F}_{qm}\), length \(n \leq m\), cardinality \(M\), minimum rank distance \(d\)

\(\tau < d\)

Find lower and upper bound on

\[
\ell \overset{\text{def}}{=} \ell(m, n, d, \tau) \overset{\text{def}}{=} \max_{\mathbf{r} \in \mathbb{F}_q^{nm}} \{|C \cap B_{\tau}(\mathbf{r})|\}
\]

- Lower exponential bound: no polynomial-time list decoding
- Upper polynomial bound: possibly polynomial-time list decoding
1 Rank-Metric Codes & Decoding Principles

2 Problem Statement

3 A Bound on the List Size of Gabidulin Codes
   - Lower Bound
   - Asymptotic Behavior of Bounds

4 Bounds for General Rank-Metric Codes
   - Interpretation as Constant-Rank Code
   - Upper Bound
   - Lower Bound
   - Asymptotic Behavior of Bounds

5 Conclusion & Outlook
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 \( r \in \mathbb{F}_{q^m}^n \) such that

\[
\ell \geq |\text{Gab}[n, k] \cap B_\tau(r)| \geq \frac{\left\lceil \frac{n}{n-\tau} \right\rceil}{(q^m)^{n-\tau-k}} \geq q^m q^{\tau(m+n)-\tau^2-md}
\]

- For \( n = m \): \( \ell \geq q^n(1-\epsilon) \cdot q^{2n\tau-\tau^2-nd+n\epsilon} \)
- Exponential in \( n \) if \( \tau \geq n - \sqrt{n(n - d + \epsilon)} \) and \( 0 \leq \epsilon < 1 \) 
  (\( = \) Johnson radius)
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 \( r \in \mathbb{F}_{q^m}^n \) such that

\[
\ell \geq |\text{Gab}[n, k] \cap B_{\tau}(r)| \geq \frac{\left[ \frac{n}{n-\tau} \right]}{(q^m)^{n-\tau-k}} \geq q^m q^{\tau(m+n)-\tau^2-md}
\]

- For \( n = m \): \( \ell \geq q^{n(1-\epsilon)} \cdot q^{2n\tau-\tau^2-md+n\epsilon} \)
- Exponential in \( n \) if \( \tau \geq n - \sqrt{n(n - d + \epsilon)} \) and \( 0 \leq \epsilon < 1 \) 
  (\( = \) Johnson radius)
Lower Bound for Gabidulin Codes – Sketch of Proof

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

- $\mathcal{P}^* \overset{\text{def}}{=} \text{set of all monic linearized polynomials of } \deg_q = n - \tau \text{ and a root space over } \mathbb{F}_{q^n} \text{ of dimension } n - \tau > k - 1$
  $\implies |\mathcal{P}^*| = \begin{pmatrix} n \\ n-\tau \end{pmatrix}$

- $\mathcal{P} \subset \mathcal{P}^*$, s.t. all $q$-monomials of $\deg_q \geq k$ have same coefficients

- pigeonhole principle: There exist coefficients s.t. $|\mathcal{P}| \geq \begin{pmatrix} n \\ n-\tau \end{pmatrix} \frac{1}{(q^m)^{n-\tau-k}}$
  $\implies$ For all $f(x), g(x) \in \mathcal{P} \implies \deg_q(f(x) - g(x)) < k$

- let $r$ be the evaluation of $f(x)$ at a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$

- let $c$ be the evaluation of $f(x) - g(x)$ at this basis
  $\implies r - c$ is the evaluation of $f(x) - f(x) + g(x) = g(x) \in \mathcal{P}$
  $\implies \dim \ker(r - c) = n - \tau \iff \rk(r - c) = \tau$

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 $\tau$ from $r$.

$\implies \ell \geq |\mathcal{P}|$
Sketch of proof: (Similar to Justesen & Høholdt and Ben-Sasson, Kopparty & Radhakrishnan for RS codes)

- $\mathcal{P}^\ast \overset{\text{def}}{=} \text{set of all monic linearized polynomials of } \deg_q = n - \tau \text{ and a root space over } \mathbb{F}_{q^n} \text{ of dimension } n - \tau > k - 1$
  $\implies |\mathcal{P}^\ast| = \left[ \frac{n}{n - \tau} \right]$

- $\mathcal{P} \subseteq \mathcal{P}^\ast$, s.t. all $q$-monomials of $\deg_q \geq k$ have same coefficients

- pigeonhole principle: There exist coefficients s.t. $|\mathcal{P}| \geq \frac{n}{(q^m)^{n - \tau - k}}$
  $\implies$ For all $f(x), g(x) \in \mathcal{P} \implies \deg_q(f(x) - g(x)) < k$

- let $r$ be the evaluation of $f(x)$ at a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$

- let $c$ be the evaluation of $f(x) - g(x)$ at this basis
  $\implies r - c$ is the evaluation of $f(x) - f(x) + g(x) = g(x) \in \mathcal{P}$
  $\implies \dim \ker(r - c) = n - \tau \iff \text{rk}(r - c) = \tau$

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

$\implies \ell \geq |\mathcal{P}|$ $\square$
Sketch of proof: (Similar to Justesen & Høholdt and Ben-Sasson, Kopparty & Radhakrishnan for RS codes)

- $\mathcal{P}^* \overset{\text{def}}{=} \text{set of all monic linearized polynomials of } \deg_q = n - \tau \text{ and a root space over } \mathbb{F}_{q^n} \text{ of dimension } n - \tau > k - 1$
  $\implies |\mathcal{P}^*| = \binom{n}{n-\tau}$
- $\mathcal{P} \subset \mathcal{P}^*$, s.t. all $q$-monomials of $\deg_q \geq k$ have same coefficients
- pigeonhole principle: There exist coefficients s.t. $|\mathcal{P}| \geq \frac{n}{(q^m)^{n-\tau-k}}$
  $\implies$ For all $f(x), g(x) \in \mathcal{P} \implies \deg_q(f(x) - g(x)) < k$
- let $r$ be the evaluation of $f(x)$ at a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$
- let $c$ be the evaluation of $f(x) - g(x)$ at this basis
  $\implies r - c$ is the evaluation of $f(x) - f(x) + g(x) = g(x) \in \mathcal{P}$
  $\implies \dim \ker(r - c) = n - \tau \iff \rk(r - c) = \tau$

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

$\implies \ell \geq |\mathcal{P}|$ \hspace{1cm} $\square$
Sketch of proof: (Similar to Justesen & Høholdt and Ben-Sasson, Kopparty & Radhakrishnan for RS codes)

- \( \mathcal{P}^* \) def set of all monic linearized polynomials of \( \deg_q = n - \tau \) and a root space over \( \mathbb{F}_{q^n} \) of dimension \( n - \tau > k - 1 \)

\[ \Rightarrow |\mathcal{P}^*| = \begin{bmatrix} n \\ n - \tau \end{bmatrix} \]

- \( \mathcal{P} \subset \mathcal{P}^* \), s.t. all \( q \)-monomials of \( \deg_q \geq k \) have same coefficients

- pigeonhole principle: There exist coefficients s.t. \( |\mathcal{P}| \geq \frac{n}{(q^m)^{n - \tau - k}} \)

\[ \Rightarrow \text{For all } f(x), g(x) \in \mathcal{P} \Rightarrow \deg_q (f(x) - g(x)) < k \]

- let \( r \) be the evaluation of \( f(x) \) at a basis of \( \mathbb{F}_{q^n} \) over \( \mathbb{F}_q \)

- let \( c \) be the evaluation of \( f(x) - g(x) \) at this basis

\[ \Rightarrow r - c \text{ is the evaluation of } f(x) - f(x) + g(x) = g(x) \in \mathcal{P} \]
\[ \Rightarrow \text{dim ker}(r - c) = n - \tau \iff \text{rk}(r - c) = \tau \]

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 \( \tau \) from \( r \).

\[ \Rightarrow \ell \geq |\mathcal{P}| \]

\[ \square \]
Asymptotic Behavior of Bounds on the List Size

Reed–Solomon Codes

Gabidulin Codes

- Different behavior?
- Are the unknown regions somehow connected?
Outline

1. Rank-Metric Codes & Decoding Principles
2. Problem Statement
3. A Bound on the List Size of Gabidulin Codes
   - Lower Bound
   - Asymptotic Behavior of Bounds
4. Bounds for General 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:
\[ \mathcal{L} = \{c_0, c_1, \ldots, c_{\ell-1}\} = C \cap B_\tau(r) = \sum_{i=0}^\tau (C \cap S_i(r)) \]

- Consider codewords \( c_0, c_1, \ldots, c_{\ell-1} \) in distance exactly \( \tau \)
- Define \( \overline{\mathcal{L}} = \{r - c_0, \ldots, r - c_{\ell-1}\} \)
- \( \text{rk}(r - c_i - (r - c_j)) = \text{rk}(c_j - c_i) \geq d \implies \overline{\mathcal{L}} \) is a constant-rank code of rank \( \tau \) and min. distance \( \geq d \)
- \( |C \cap S_\tau(r)| \leq A_{qm}^R (n, d_R \geq d, \tau) \)

\[ \implies \text{Bounds on the cardinality of constant-rank codes can be used for bounding the list size!} \]
Interpretation as Constant-Rank Code

decoding list:
\[ \mathcal{L} = \{c_0, c_1, \ldots, c_{\ell-1}\} = C \cap B_\tau(r) = \sum_{i=0}^\tau (C \cap S_i(r)) \]

- Consider codewords \( c_0, c_1, \ldots, c_{\ell-1} \) in distance exactly \( \tau \)
- Define \( \overline{\mathcal{L}} = \{r - c_0, \ldots, r - c_{\ell-1}\} \)
- \( \operatorname{rk}(r - c_i - (r - c_j)) = \operatorname{rk}(c_j - c_i) \geq d \)

\[ \implies \overline{\mathcal{L}} \text{ is a constant-rank code of rank } \tau \text{ and min. distance } \geq d \]

- \( |C \cap S_\tau(r)| \leq A_{qm}^R(n, d_R \geq d, \tau) \)

\[ \implies \text{Bounds on the cardinality of constant-rank codes can be used for bounding the list size!} \]
Interpretation as Constant-Rank Code

Consider codewords $c_0, c_1, \ldots, c_{\ell-1}$ in distance exactly $\tau$

Define $\overline{L} = \{r - c_0, \ldots, r - c_{\ell-1}\}$

$\text{rk}(r - c_i - (r - c_j)) = \text{rk}(c_j - c_i) \geq d$  
$\implies \overline{L}$ is a constant-rank code of rank $\tau$ and min. distance $\geq d$

$|C \cap S_{\tau}(r)| \leq A_{q^m}^{R} (n, d_R \geq d, \tau)$

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

decoding list:
$L = \{c_0, c_1, \ldots, c_{\ell-1}\} = C \cap B_{\tau}(r) = \sum_{i=0}^{\tau} (C \cap S_i(r))$
Theorem (Bound II: Upper Bound for any Rank-Metric Code)

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

$$\ell = \max_{r \in \mathbb{F}_q^m} \left\{ |C \cap B_\tau(r)| \right\} \leq 1 + \sum_{t=\lfloor \frac{d-1}{2} \rfloor + 1}^{\tau} \frac{\left\lfloor \frac{n}{2t+1-d} \right\rfloor}{\left\lfloor \frac{t}{2t+1-d} \right\rfloor}$$

$$\leq 1 + 4 \cdot (\tau - \left\lfloor \frac{d-1}{2} \right\rfloor) \cdot q^{(2\tau-d+1)(n-\lfloor (d-1)/2 \rfloor-1)}$$

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

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

\[
\ell = \max_{r \in \mathbb{F}_q^n} \left\{ |C \cap B_\tau(r)| \right\} \leq 1 + \sum_{t=\lceil \frac{d-1}{2} \rceil + 1}^{\tau} \frac{n}{\lceil \frac{2t+1-d}{2t+1-d} \rceil} \\
\leq 1 + 4 \cdot (\tau - \lceil \frac{d-1}{2} \rceil) \cdot q^{(2\tau-d+1)(n-\lceil (d-1)/2 \rceil-1)}
\]

- Exponential in \( n \leq m \) for any \( \tau > \lceil (d-1)/2 \rceil \)
- Does not provide any conclusion if polynomial-time list decoding is possible or not...
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 \( r \in \mathbb{F}_{q^m}^n \) such that

\[
\ell = \ell(m, n, d, \tau) \geq |C \cap B_\tau(r)| \geq q^{(n-\tau)(\tau-\lfloor (d-1)/2 \rfloor)}.
\]

- 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 always 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 \( \lfloor \frac{(d-1)}{2} \rfloor \leq \tau < d \leq n \leq m \) and \( \tau \leq n - \tau \).

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

\[
\ell = \ell(m, n, d, \tau) \geq |C \cap B_\tau(r)| \geq q^{(n-\tau)(\tau - \lfloor \frac{(d-1)}{2} \rfloor)}.
\]

- There exists a rank-metric code such that max. list size is **exponential** in \( n \) for \( \tau > \lfloor \frac{(d-1)}{2} \rfloor \).
  \( \Longrightarrow \) No polynomial-time list decoding for these codes!

- \( C \) might be non-linear and non-MRD

- \( \tau \leq n - \tau \) is always fulfilled for \( \tau = \lfloor \frac{(d-1)}{2} \rfloor + 1 \) and \( k > 1 \)
Theorem (Bound III: Lower Bound for some Rank-Metric Code)

Let \( \lceil (d-1)/2 \rceil \leq \tau < d \leq n \leq m \) and \( \tau \leq n - \tau \). Then, there exists an \((n, M, d_R \geq d)\) code \( C \) over \( \mathbb{F}_{q^m} \) and a word \( r \in \mathbb{F}_{q^m} \) such that

\[
\ell = \ell(m, n, d, \tau) \geq |C \cap B_\tau(r)| \geq q^{(n-\tau)(\tau - \lceil (d-1)/2 \rceil)}.
\]

- There exists a rank-metric code such that max. list size is **exponential** in \( n \) for \( \tau > \lceil (d-1)/2 \rceil \).
  \( \implies \) No polynomial-time list decoding for these codes!
- \( C \) might be non-linear and non-MRD
- \( \tau \leq n - \tau \) is always fulfilled for \( \tau = \lceil (d-1)/2 \rceil + 1 \) and \( k > 1 \)
Sketch of Proof:

- Use two constant-dimension codes (lifted MRD codes) to construct
  - A CR\(_{q^m}(n, M, d_R \geq d, \tau)\) constant-rank code
  - With cardinality \(q^{(n-\tau)(\tau-[\frac{(d-1)}{2}])}\)

Denote the codewords of this constant-rank code by \(\{a_0, a_1, \ldots\}\).

- Choose \(r = 0\):
  - \(rk(r - a_i) = rk(a_i) = \tau\) for all \(i\) (constant-rank code)
  - \(d_R(a_i, a_j) = rk(a_i - a_j) \geq d\)

\(\Rightarrow a_0, a_1, \ldots\) are codewords of a code with rank distance at least \(d\)
\(\Rightarrow\) and lie all on a sphere of radius \(\tau\) around \(r\).

There exists a \((n, M, d_R \geq d)_R\) code \(C\) of min. rank distance at least \(d\)
s.t. \(\ell \geq |C \cap S_\tau(r)| = |CR| = q^{(n-\tau)(\tau-[\frac{(d-1)}{2}])}\).
\(\square\)
Lower Bound for Rank Metric Codes — Sketch of Proof

Sketch of Proof:

- Use two constant-dimension codes (lifted MRD codes) to construct
  - a CR\(q^m(n, M, d_R \geq d, \tau)\) constant-rank code
  - with cardinality \(q^{(n-\tau)(\tau-\lfloor(d-1)/2\rfloor)}\)

Denote the codewords of this constant-rank code by \(\{a_0, a_1, \ldots\}\).

- Choose \(r = 0\):
  - \(rk(r - a_i) = rk(a_i) = \tau\) for all \(i\) (constant-rank code)
  - \(d_R(a_i, a_j) = rk(a_i - a_j) \geq d\)

\[\Rightarrow a_0, a_1, \ldots\text{ are codewords of a code with rank distance at least } d\]
\[\Rightarrow\text{ and lie all on a sphere of radius } \tau\text{ around } r\]

There exists a \((n, M, d_R \geq d)_R\) code \(C\) of min. rank distance at least \(d\)
s.t. \(\ell \geq |C \cap S_\tau(r)| = |CR| = q^{(n-\tau)(\tau-\lfloor(d-1)/2\rfloor)}\).
Sketch of Proof:

- Use two constant-dimension codes (lifted MRD codes) to construct a $\text{CR}_{q^m}(n, M, d_R \geq d, \tau)$ constant-rank code with cardinality $q^{(n-\tau)(\tau-\lceil(d-1)/2\rceil)}$.

Denote the codewords of this constant-rank code by $\{a_0, a_1, \ldots\}$.

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

  $\Rightarrow a_0, a_1, \ldots$ are codewords of a code with rank distance at least $d$ and lie all on a sphere of radius $\tau$ around $r$.

There exists a $(n, M, d_R \geq d)_R$ code $C$ of min. rank distance at least $d$ s.t. $\ell \geq |C \cap S_\tau(r)| = |\text{CR}| = q^{(n-\tau)(\tau-\lceil(d-1)/2\rceil)}$.  

Sketch of Proof:

- Use two constant-dimension codes (lifted MRD codes) to construct
  - a CR$^{m}(n, M, d_R \geq d, \tau)$ constant-rank code
  - with cardinality $q^{(n-\tau)(\tau-[\frac{(d-1)}{2}])}$

Denote the codewords of this constant-rank code by $\{a_0, a_1, \ldots\}$.

- Choose $r = 0$:
  - $rk(r - a_i) = rk(a_i) = \tau$ for all $i$ (constant-rank code)
  - $d_R(a_i, a_j) = rk(a_i - a_j) \geq d$

  $\Rightarrow a_0, a_1, \ldots$ are codewords of a code with rank distance at least $d$
  $\Rightarrow$ and lie all on a sphere of radius $\tau$ around $r$

There exists a $(n, M, d_R \geq d)_R$ code $C$ of min. rank distance at least $d$

s.t. $\ell \geq |C \cap S_{\tau}(r)| = |CR| = q^{(n-\tau)(\tau-[\frac{(d-1)}{2}])}$. 

\[\square\]
Asymptotic Behavior of Bounds on the List Size

**Codes in Hamming Metric**

- There is a code with **exponential** list size
- There is a code with polynomial list size
- There is a code with **unique** list size

**Codes in Rank Metric**

- There is a code with exponential list size
- There is a code with polynomial list size
- There is a code with unique list size

- Behavior is different
- There exists **no polynomial upper bound** in rank metric, depending only on $n$ and $d$, as the Johnson bound in Hamming metric!
Outline

1. Rank-Metric Codes & Decoding Principles
2. Problem Statement
3. A Bound on the List Size of Gabidulin Codes
   - Lower Bound
   - Asymptotic Behavior of Bounds
4. Bounds for General 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 problem: find bound up to Johnson radius!

Upper bound for any rank-metric code: 
- exponential in \( n \) for \( \tau > \lfloor (d-1)/2 \rfloor \)

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-time Johnson-like upper bound
- open problem: prove sth. similar for 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 problem:** find bound up to Johnson radius!

Upper bound for **any** rank-metric code:
- exponential in \( n \) for \( \tau > \lfloor (d-1)/2 \rfloor \)

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-time Johnson-like upper bound
- **open problem:** prove sth. similar for **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 problem:** find bound up to Johnson radius!

Upper bound for **any** rank-metric code:
- exponential in $n$ for $\tau > \lceil (d-1)/2 \rceil$

Lower bound for rank-metric codes:
- there exists a rank-metric code with exponential list size for **any** $\tau > \lceil (d-1)/2 \rceil$
- there is no polynomial-time Johnson-like upper bound
- **open problem:** prove sth. similar for **linear** rank-metric codes!
Thank you...

...for your attention!
Sketch of Proof:

- $\overline{L}_t = C \cap S_t(r) = \{r - c_1, \ldots, r - c_\ell\}$
  $\implies \overline{L}_t$ is a $\text{CR}_{q^m}(n, M, d_R \geq d, t)$ constant-rank code

- Use maximum cardinality of such a CRC as upper bound:
  $|C \cap S_t(r)| \leq A_{q^m}^R(n, d_R \geq d, t) \leq A_{q^m}^R(n, d, t)$

- Use connection between CRCs and constant-dimension codes (CDCs), see [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 CDCs by [Wang, Xing, Safavi-Naini, 2003]:
  $A_q^S(n, d_S = 2(d - t), t) \leq \left\lceil \frac{n}{t - (d - t) + 1} \right\rceil$.

Summing up for $t = \left\lfloor \frac{(d-1)}{2} \right\rfloor + 1, \ldots, \tau$ gives the statement. $\square$
Sketch of Proof:

- $\overline{L}_t = C \cap S_t(r) = \{r - c_1, \ldots, r - c_\ell\}$
  $\implies \overline{L}_t$ is a $\text{CR}_{q^m}(n, M, d_R \geq d, t)$ constant-rank code

- Use maximum cardinality of such a CRC as upper bound:
  $|C \cap S_t(r)| \leq A_{q^m}^R (n, d_R \geq d, t) \leq A_{q^m}^R (n, d, t)$

- Use connection between CRCs and constant-dimension codes (CDCs), see [Gadouleau, Yan, 2010]:
  $A_{q^m}^R (n, d, t) \leq A_{q^S}^S (n, d_S = 2(d - t), t)$

- Use upper bound on cardinality of CDCs by [Wang, Xing, Safavi-Naini, 2003]:
  $A_{q^S}^S (n, d_S = 2(d - t), t) \leq \left[\frac{n}{t-(d-t)+1}\right]_{\left[\frac{t-(d-t)+1}{t-(d-t)+1}\right]}$.

Summing up for $t = \lfloor (d-1)/2 \rfloor + 1, \ldots, \tau$ gives the statement.
Sketch of Proof:

- \( \overline{L}_t = C \cap S_t(r) = \{r - c_1, \ldots, r - c_\ell\} \)
  \( \implies \overline{L}_t \) is a \( CR_{q^m} (n, M, d_R \geq d, t) \) constant-rank code

- Use maximum cardinality of such a CRC as upper bound:
  \( |C \cap S_t(r)| \leq A_{q^m}^R (n, d_R \geq d, t) \leq A_{q^m}^R (n, d, t) \)

- Use connection between CRCs and constant-dimension codes (CDCs), see [Gadouleau, Yan, 2010]:
  \( A_{q^m}^R (n, d, t) \leq A_{q^S}^S (n, d_S = 2(d - t), t) \)

- Use upper bound on cardinality of CDCs by [Wang, Xing, Safavi-Naini, 2003]:
  \( A_{q^S}^S (n, d_S = 2(d - t), t) \leq \begin{bmatrix} t & n \\ \frac{(d-t)+1}{t} \\ \frac{(d-t)+1}{t} \end{bmatrix} \).

Summing up for \( t = \lfloor (d-1)/2 \rfloor + 1, \ldots, \tau \) gives the statement.
Sketch of Proof:

- \( \mathcal{L}_t = \mathcal{C} \cap \mathcal{S}_t(r) = \{r - c_1, \ldots, r - c_\ell\} \)
  \( \implies \mathcal{L}_t \) is a CR\(_q^m\) \((n, M, d_R \geq d, t)\) constant-rank code

- Use maximum cardinality of such a CRC as upper bound:
  \(|\mathcal{C} \cap \mathcal{S}_t(r)| \leq \mathcal{A}_{q^m}^R(n, d_R \geq d, t) \leq \mathcal{A}_{q^m}^R(n, d, t)\)

- Use connection between CRCs and constant-dimension codes (CDCs), see [Gadouleau, Yan, 2010]:
  \( \mathcal{A}_{q^m}^R(n, d, t) \leq \mathcal{A}_q^S(n, d_S = 2(d - t), t)\)

- Use upper bound on cardinality of CDCs by [Wang, Xing, Safavi-Naini, 2003]:
  \( \mathcal{A}_q^S(n, d_S = 2(d - t), t) \leq \left\lfloor \frac{n}{t} \right\rfloor \left\lfloor \frac{n}{t} - \frac{d - t}{d} + 1 \right\rfloor. \)

Summing up for \( t = \left\lfloor (d - 1)/2 \right\rfloor + 1, \ldots, \tau \) gives the statement.