Bounds on List Decoding of Rank-Metric Codes

Antonia Wachter-Zeh

Computer Science Departement, Technion—Israel Institute of Technology

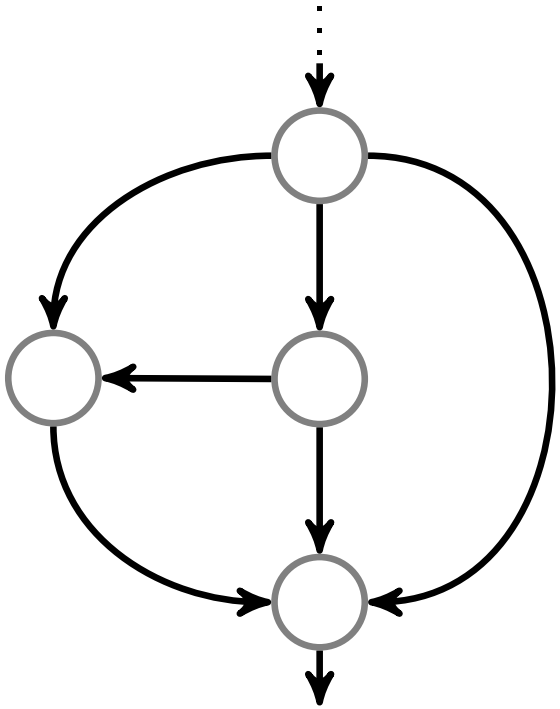
November 3, 2013

Motivation: Network Coding

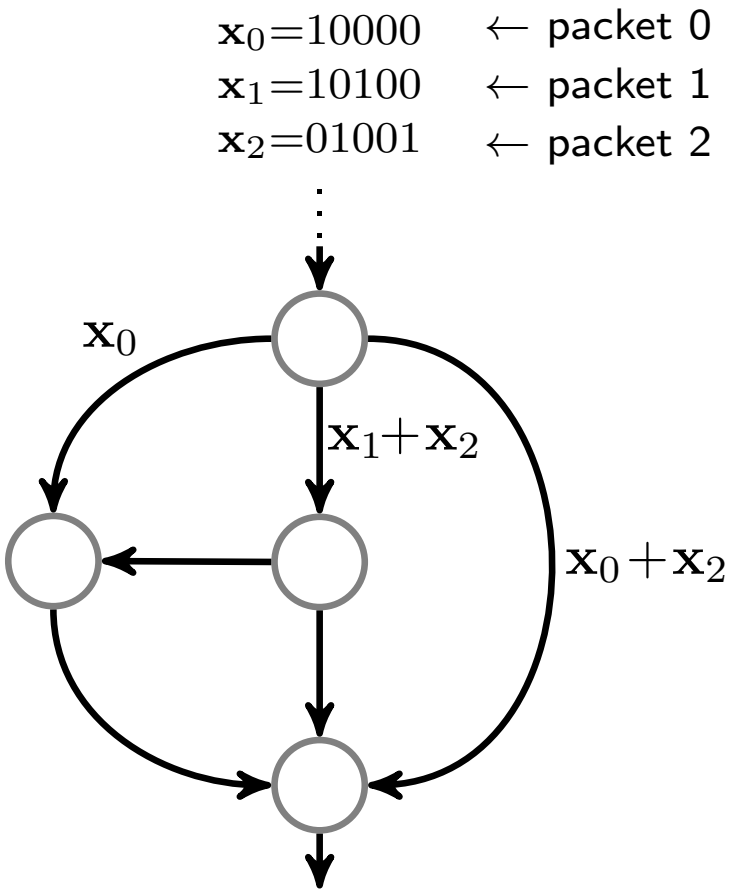
$\mathbf{x}_0 = 10000$ ← packet 0
$\mathbf{x}_1 = 10100$ ← packet 1
$\mathbf{x}_2 = 01001$ ← packet 2
$\vdots$

Motivation: Network Coding

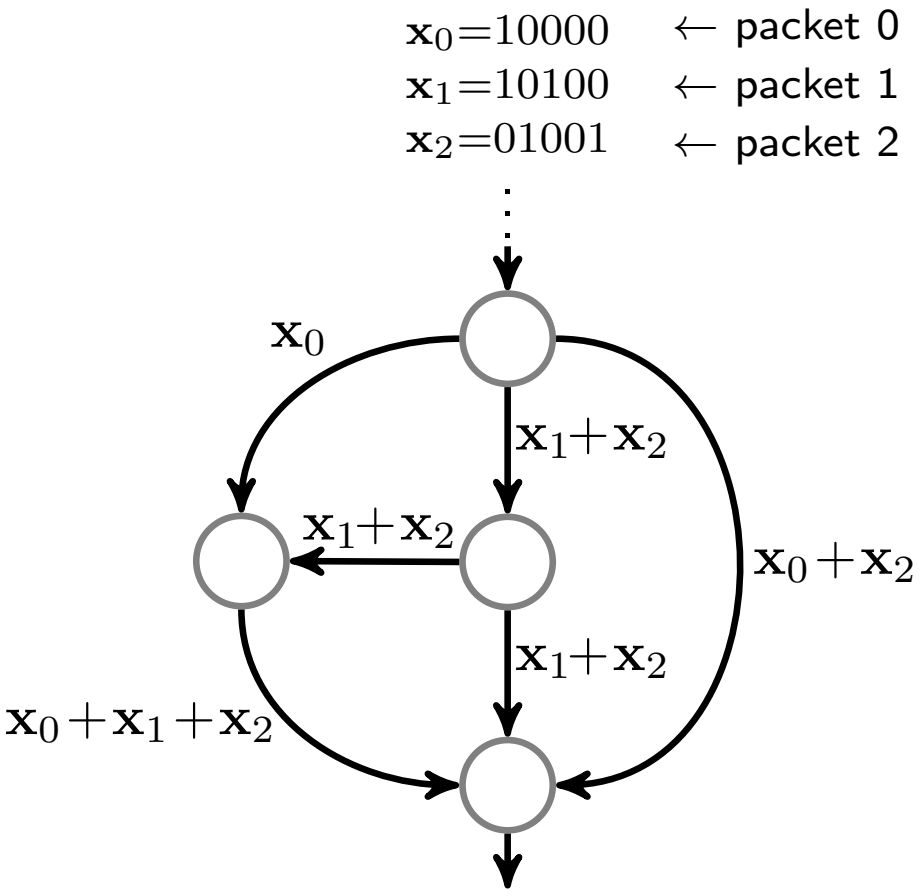
$\mathbf{x}_0 = 10000$ ← packet 0
$\mathbf{x}_1 = 10100$ ← packet 1
$\mathbf{x}_2 = 01001$ ← packet 2



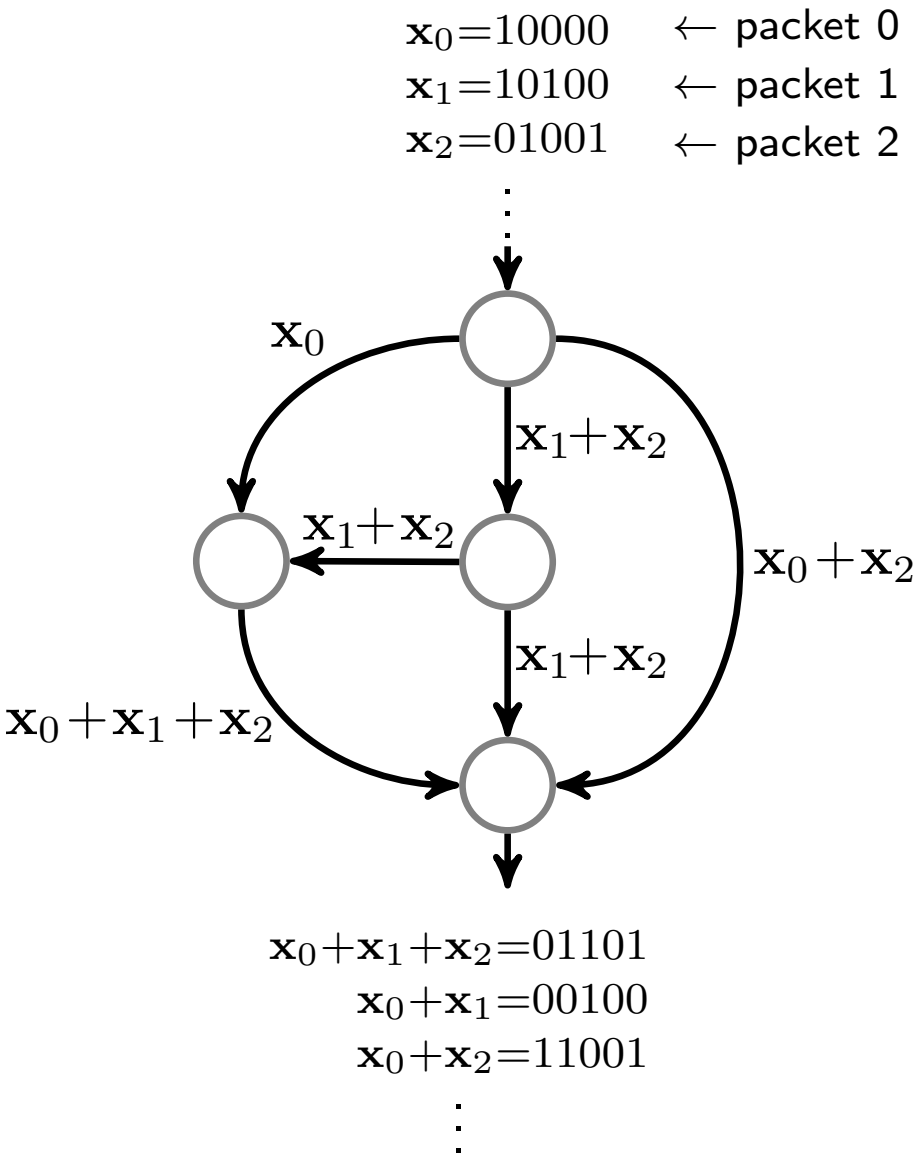
Motivation: Network Coding



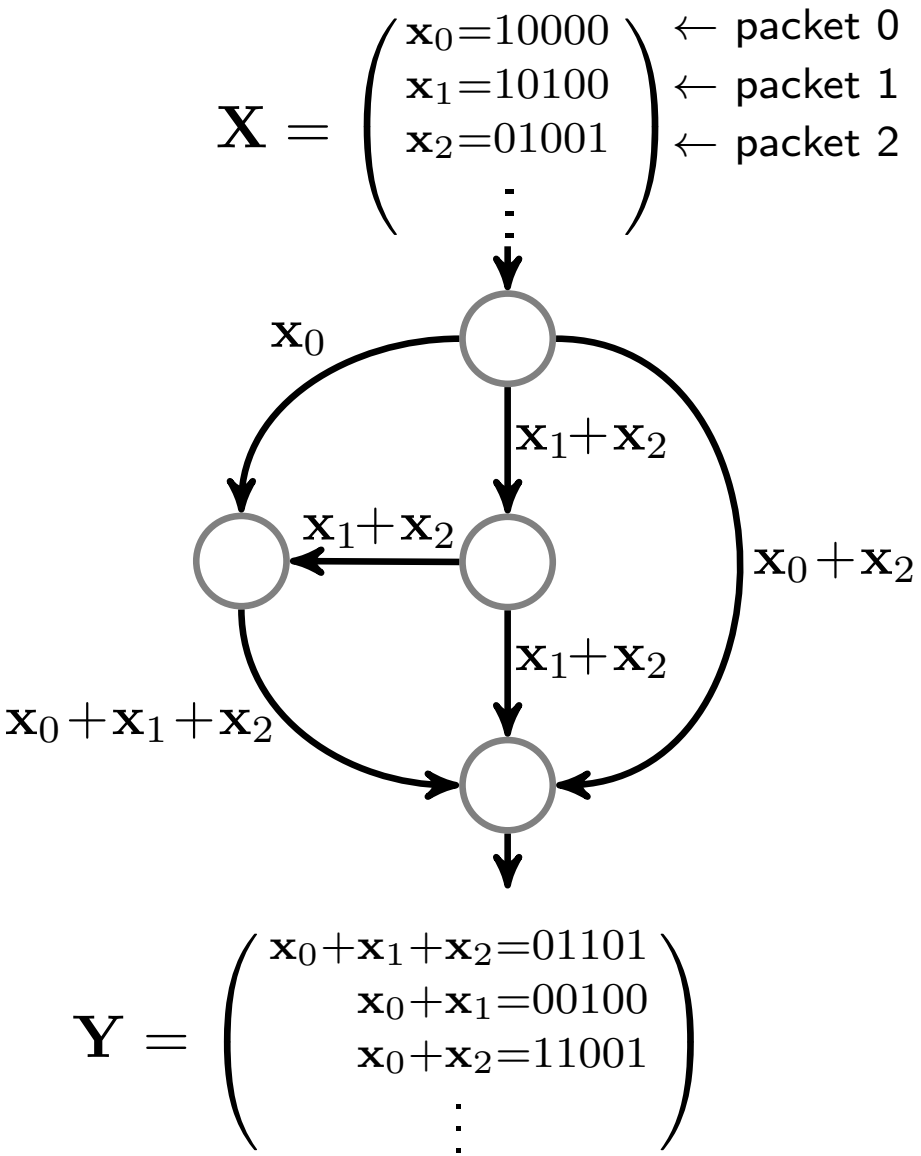
Motivation: Network Coding



Motivation: Network Coding



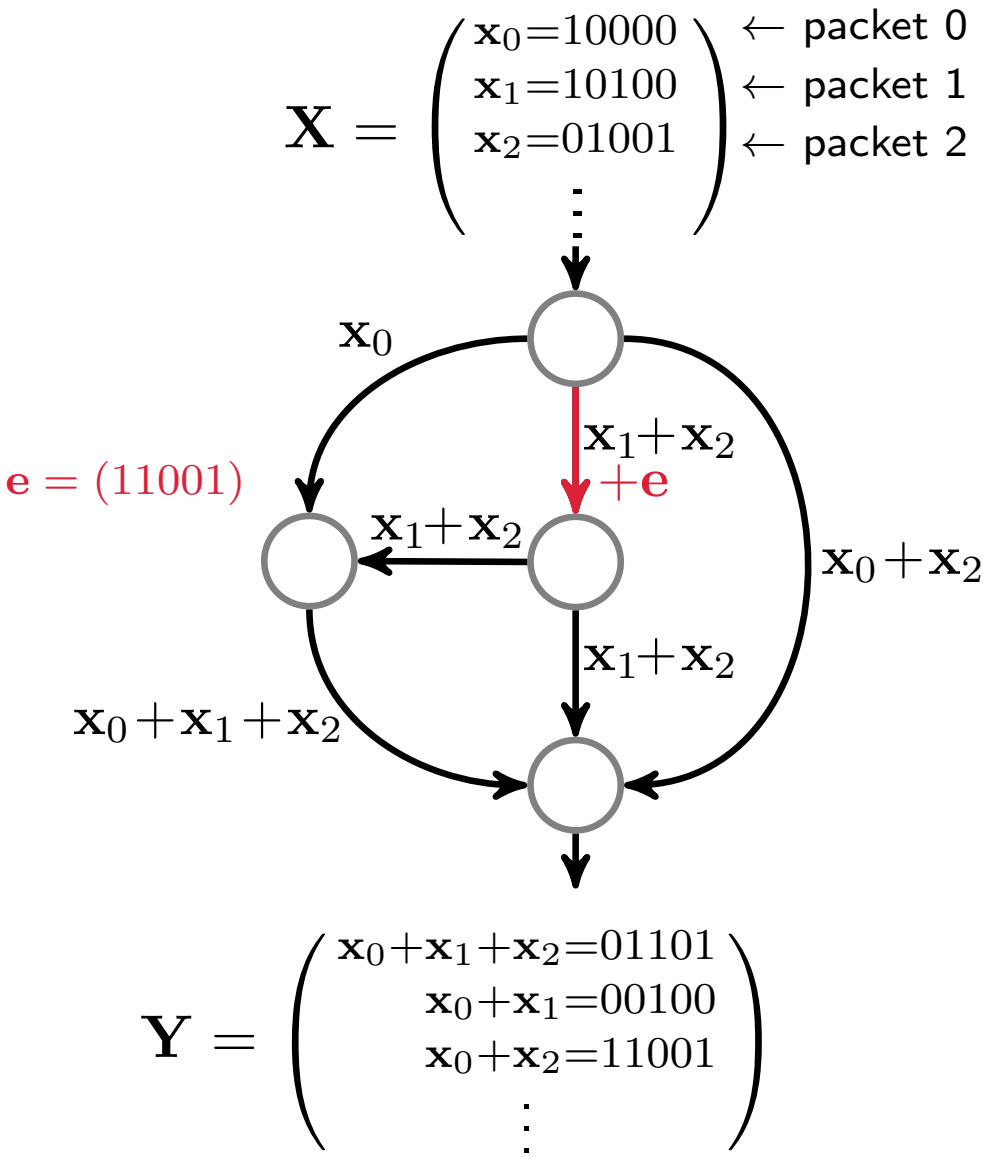
Motivation: Network Coding



- error-free:

  $\text{rowspace}(\mathbf{X}) = \text{rowspace}(\mathbf{Y})$

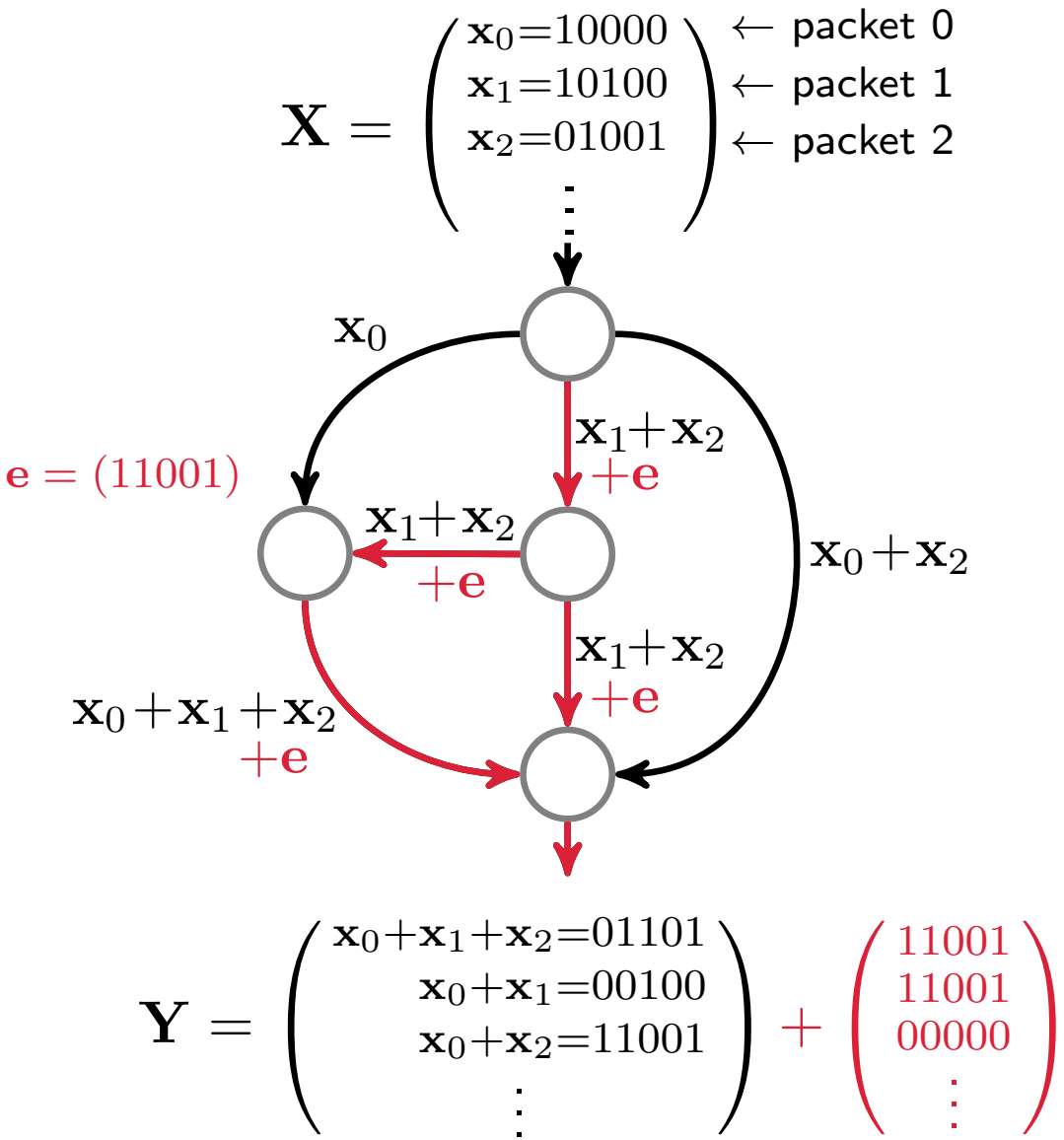
Motivation: Network Coding



- error-free:

  $\text{rowspace}(\mathbf{X}) = \text{rowspace}(\mathbf{Y})$

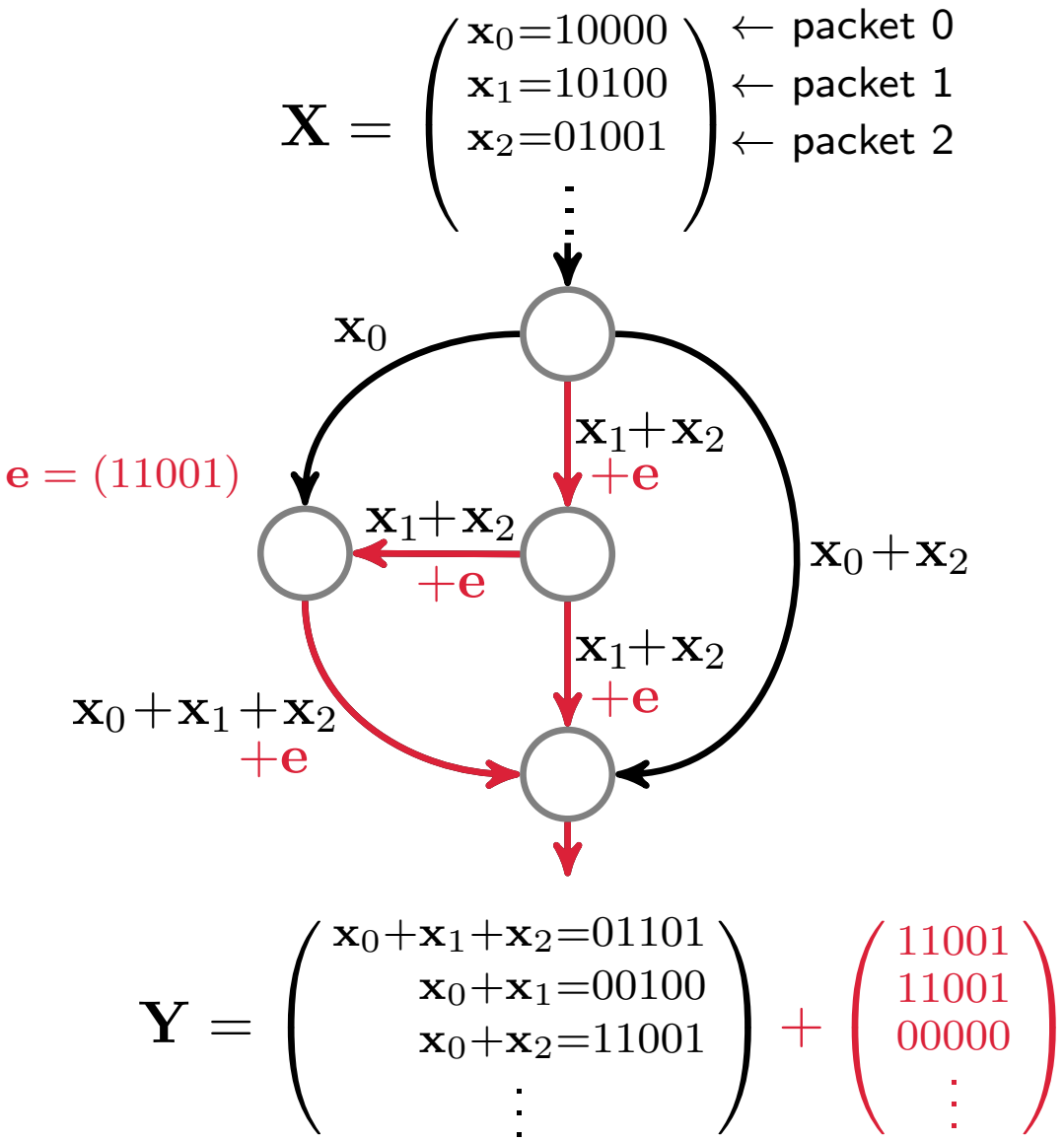
Motivation: Network Coding



- 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)
$\Longrightarrow$ use subspace & rank-metric codes

Outline

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

Outline

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 Codes

Rank Metric

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

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

- $d \stackrel{\text{def}}{=} \min\left\{ \mathrm{rk}\left(\mathbf{a} - \mathbf{b}\right) \ : \ \mathbf{a}, \mathbf{b} \in \mathsf{C}, \mathbf{a} \neq \mathbf{b} \right\}$
- $M \leq q^{\min\{n(m-d+1), m(n-d+1)\}}$
- 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 Codes

Rank Metric

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

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

- $d \stackrel{\text{def}}{=} \min \left\{ \mathrm{rk}\left(\mathbf{a} - \mathbf{b}\right) \ : \ \mathbf{a}, \mathbf{b} \in \mathsf{C}, \mathbf{a} \neq \mathbf{b} \right\}$
- $M \leq q^{\min\{n(m-d+1), m(n-d+1)\}}$
- 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: $\deg_q f(x) = d_f$

Gabidulin Codes

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

Definition (Gabidulin Code)

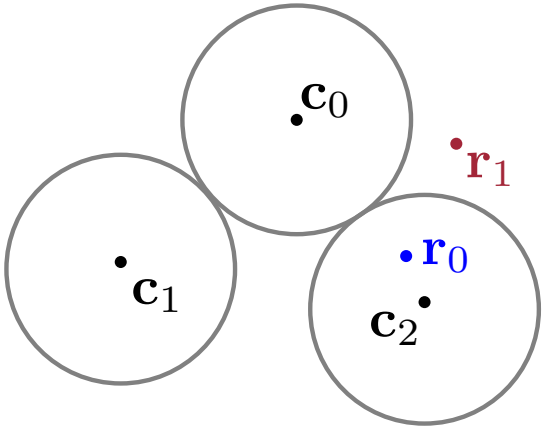
A linear Gabidulin code over $\mathbb{F}_{q^m}$ of length $n \leq m$ and dimension $k \leq n$ is defined by

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

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

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

Reed–Solomon vs. Gabidulin Codes — BMD Decoding



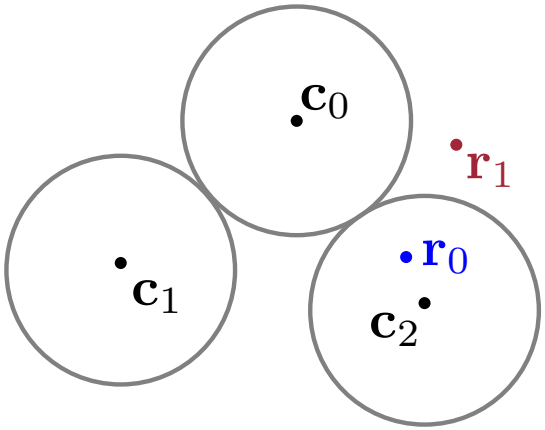
BMD decoding: $\tau = \left\lfloor \frac{d-1}{2} \right\rfloor$

$\rightarrow$ decoding result: unique or failure

Algorithms	RS Codes	Gabidulin Codes
system of equations	Peterson, Gorenstein–Zierler	Roth, Gabidulin
Euclidean algorithm	Sugiyama *et al.*, 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



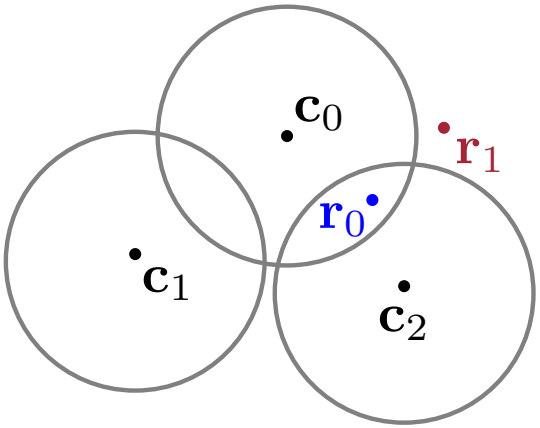
BMD decoding: $\tau = \left\lfloor \frac{d-1}{2} \right\rfloor$

$\rightarrow$ decoding result: unique or failure

Algorithms	RS Codes	Gabidulin Codes
system of equations	Peterson, Gorenstein–Zierler	Roth, Gabidulin
Euclidean algorithm	Sugiyama *et al.*, 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



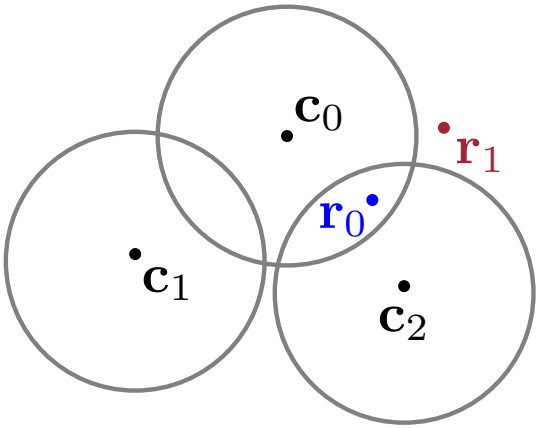
List decoding: $\tau > \left\lfloor \frac{d-1}{2} \right\rfloor$

$\rightarrow$ 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



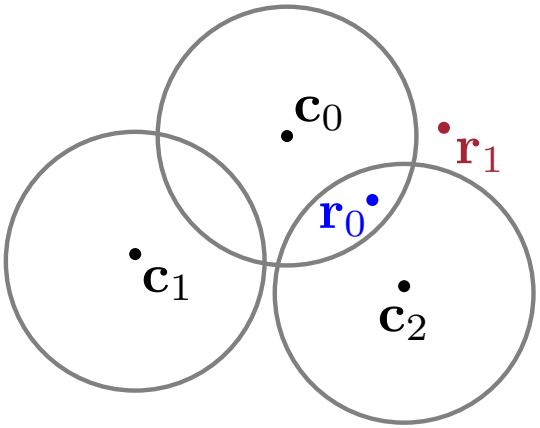
List decoding: $\tau > \left\lfloor \frac{d-1}{2} \right\rfloor$

$\rightarrow$ 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: $\tau > \left\lfloor \frac{d-1}{2} \right\rfloor$

$\rightarrow$ 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 ($\ell \leq const.$)
- *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)

Outline

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

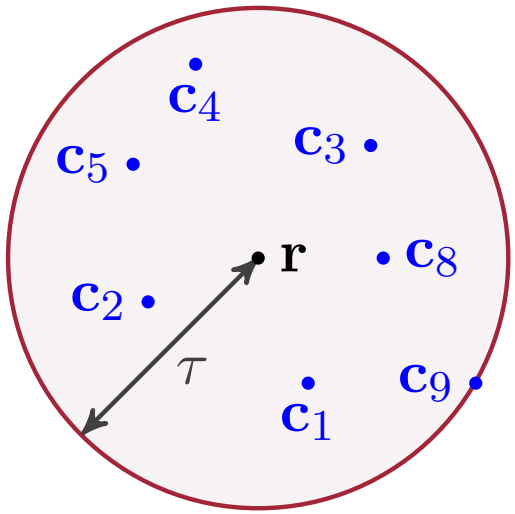
Motivation: Is **polynomial-time** list decoding possible?

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

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



→ lower exponential bound: **no** polynomial-time list decoding

→ upper polynomial bound: **maybe** polynomial-time list decoding

Motivation & Problem Statement

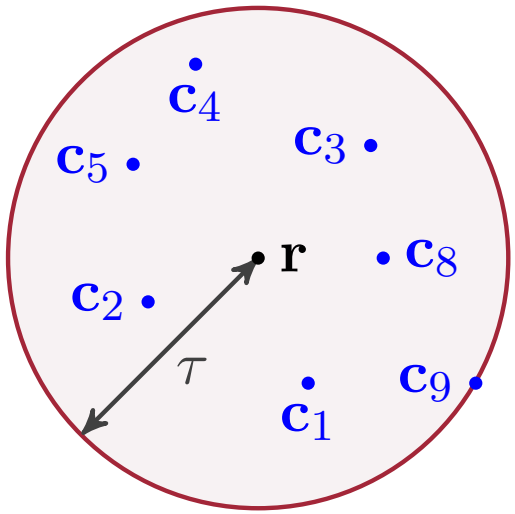
Motivation: Is **polynomial-time** list decoding possible?

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

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



$\rightarrow$ lower exponential bound: **no** polynomial-time list decoding

$\rightarrow$ upper polynomial bound: **maybe** polynomial-time list decoding

Outline

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)

- $\mathsf{Gab}[n,k]$ *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*

$$\ell \geq \left|\mathsf{Gab}[n,k] \cap \mathcal{B}_\tau(\mathbf{r})\right| \geq \frac{\begin{bmatrix} n \\ n-\tau \end{bmatrix}}{(q^m)^{n-\tau-k}} \geq q^m q^{\tau(m+n)-\tau^2-md}$$

- 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

Theorem (Bound I: Lower Bound for Gabidulin Codes)

- $\mathsf{Gab}[n,k]$ *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*

$$\ell \geq \left|\mathsf{Gab}[n,k] \cap \mathcal{B}_\tau(\mathbf{r})\right| \geq \frac{\begin{bmatrix} n \\ n-\tau \end{bmatrix}}{(q^m)^{n-\tau-k}} \geq q^m q^{\tau(m+n)-\tau^2-md}$$

- 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)

- $\mathcal{Q} \stackrel{\text{def}}{=}$ set of all monic linearized polynomials of $\deg_q = n - \tau$ and root space over $\mathbb{F}_{q^n}$ of dimension $n - \tau \implies |\mathcal{Q}| = \begin{bmatrix} n \\ n-\tau \end{bmatrix}$
- $\mathcal{P} \subset \mathcal{Q}$, s.t. all q-monomials of $\deg_q \geq k$ have same coefficients
- pigeonhole principle: There exist coefficients s.t. $|\mathcal{P}| \geq \frac{\begin{bmatrix} n \\ n-\tau \end{bmatrix}}{(q^m)^{n-\tau-k}}$
  $\implies$ 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 $f(x) - f(x) + g(x) = g(x) \in \mathcal{P}$
  $\implies \dim \ker(\mathbf{r} - \mathbf{c}) = n - \tau \iff \mathrm{rk}(\mathbf{r} - \mathbf{c}) = \tau$

Therefore, for **any** $g(x) \in \mathcal{P}$, the evaluation of $f(x) - g(x)$ is a codeword from 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)

- $\mathcal{Q} \stackrel{\text{def}}{=}$ set of all monic linearized polynomials of $\deg_q = n - \tau$ and root space over $\mathbb{F}_{q^n}$ of dimension $n - \tau \implies |\mathcal{Q}| = \begin{bmatrix} n \\ n-\tau \end{bmatrix}$
- $\mathcal{P} \subset \mathcal{Q}$, s.t. all q-monomials of $\deg_q \geq k$ have same coefficients
- pigeonhole principle: There exist coefficients s.t. $|\mathcal{P}| \geq \frac{\begin{bmatrix} n \\ n-\tau \end{bmatrix}}{(q^m)^{n-\tau-k}}$
  $\implies$ 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 $f(x) - f(x) + g(x) = g(x) \in \mathcal{P}$
  $\implies \dim \ker(\mathbf{r} - \mathbf{c}) = n - \tau \iff \mathrm{rk}(\mathbf{r} - \mathbf{c}) = \tau$

Therefore, for **any** $g(x) \in \mathcal{P}$, the evaluation of $f(x) - g(x)$ is a codeword from 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)

- $\mathcal{Q} \stackrel{\text{def}}{=}$ set of all monic linearized polynomials of $\deg_q = n - \tau$ and root space over $\mathbb{F}_{q^n}$ of dimension $n - \tau \implies |\mathcal{Q}| = \begin{bmatrix} n \\ n-\tau \end{bmatrix}$
- $\mathcal{P} \subset \mathcal{Q}$, s.t. all q-monomials of $\deg_q \geq k$ have same coefficients
- pigeonhole principle: There exist coefficients s.t. $|\mathcal{P}| \geq \frac{\begin{bmatrix} n \\ n-\tau \end{bmatrix}}{(q^m)^{n-\tau-k}}$
  $\implies$ 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 $f(x) - f(x) + g(x) = g(x) \in \mathcal{P}$
  $\implies \dim \ker(\mathbf{r} - \mathbf{c}) = n - \tau \iff \mathrm{rk}(\mathbf{r} - \mathbf{c}) = \tau$

Therefore, for **any** $g(x) \in \mathcal{P}$, the evaluation of $f(x) - g(x)$ is a codeword from 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)

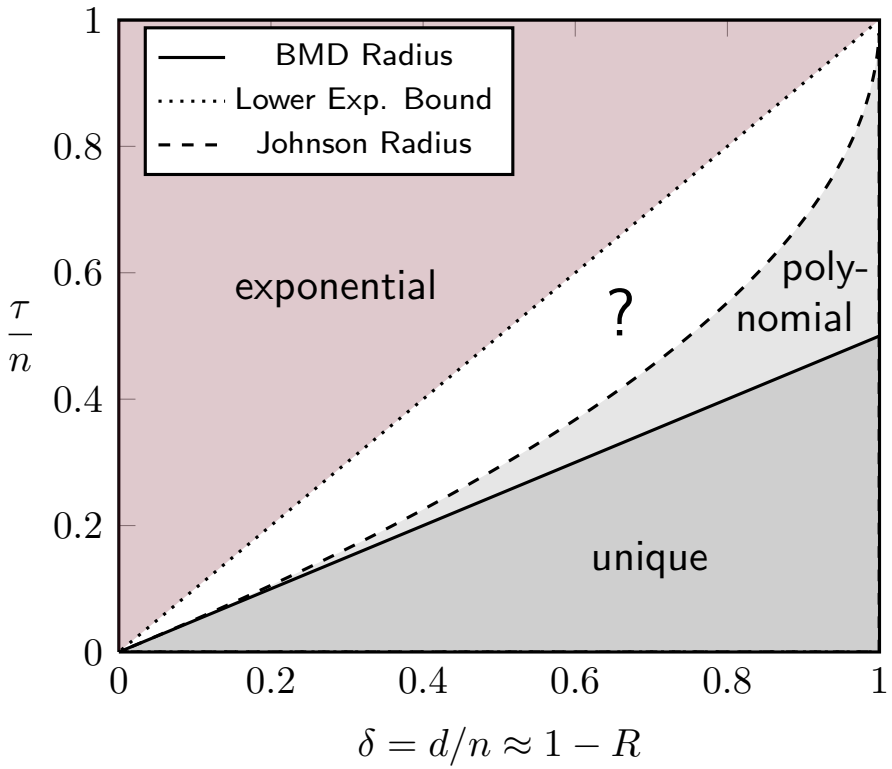
- $\mathcal{Q} \stackrel{\text{def}}{=}$ set of all monic linearized polynomials of $\deg_q = n - \tau$ and root space over $\mathbb{F}_{q^n}$ of dimension $n - \tau \implies |\mathcal{Q}| = \begin{bmatrix} n \\ n-\tau \end{bmatrix}$
- $\mathcal{P} \subset \mathcal{Q}$, s.t. all q-monomials of $\deg_q \geq k$ have same coefficients
- pigeonhole principle: There exist coefficients s.t. $|\mathcal{P}| \geq \frac{\begin{bmatrix} n \\ n-\tau \end{bmatrix}}{(q^m)^{n-\tau-k}}$
  $\implies$ 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 $f(x) - f(x) + g(x) = g(x) \in \mathcal{P}$
  $\implies \dim \ker(\mathbf{r} - \mathbf{c}) = n - \tau \iff \mathrm{rk}(\mathbf{r} - \mathbf{c}) = \tau$

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

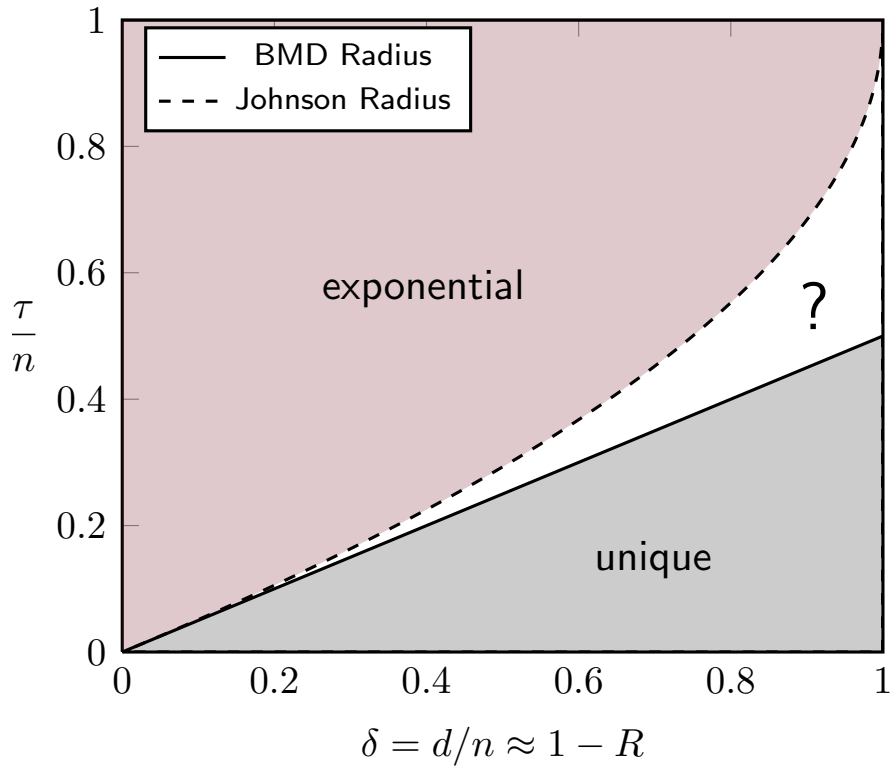
$\implies \ell \geq |\mathcal{P}|$ $\square$

Asymptotic Behavior of Bounds on the List Size

Reed–Solomon codes



Gabidulin codes

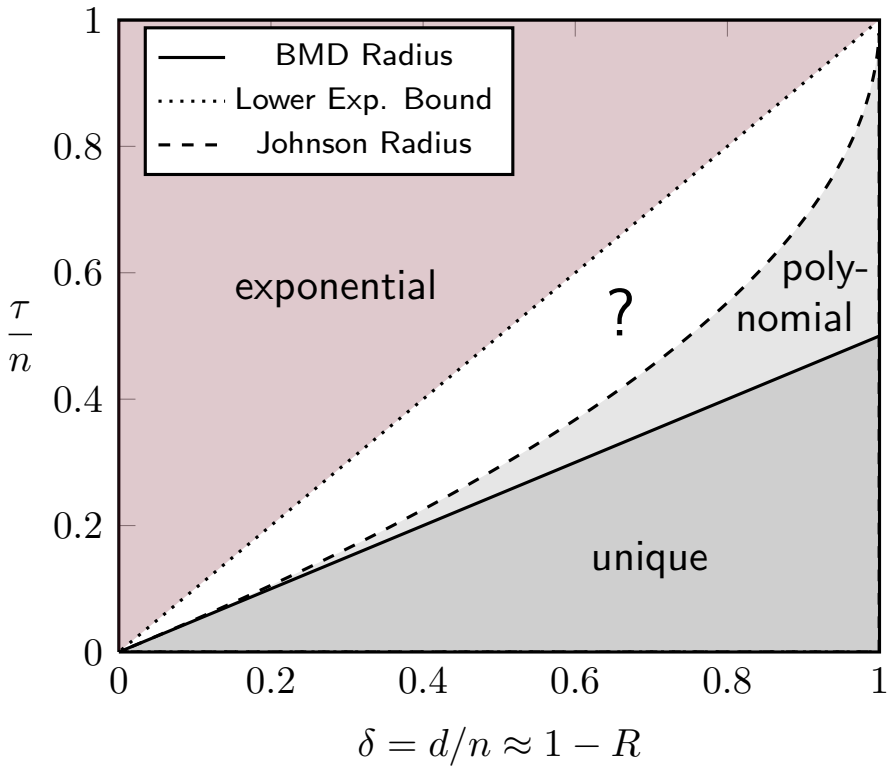


- different behavior?
- connect unknown regions?

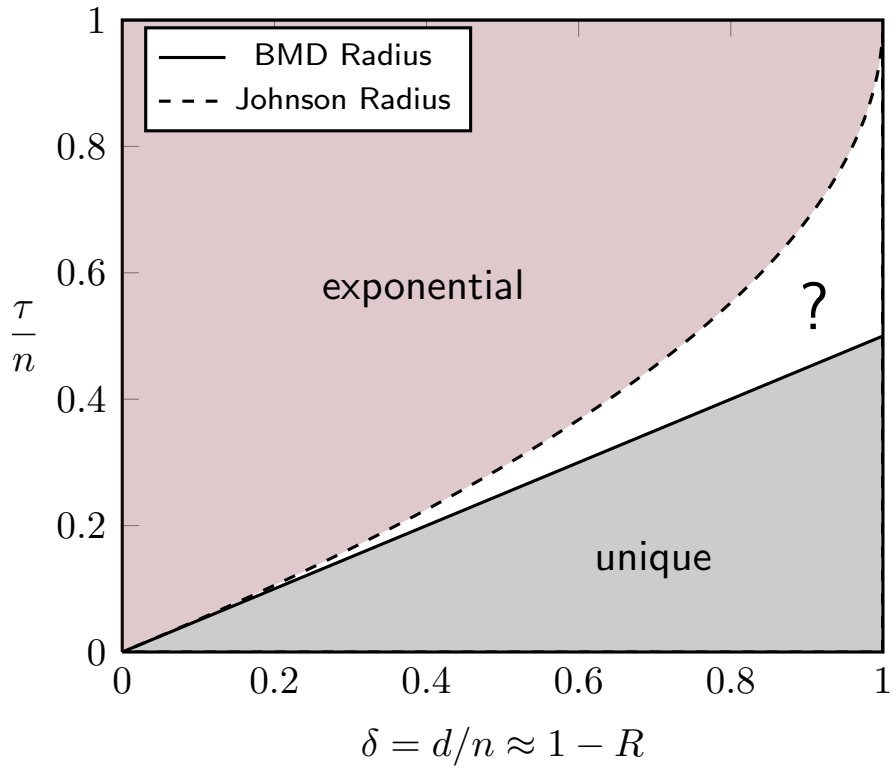
Remark: *Rudra & Wootters (Oct. 2013)*: many RS codes are list decodable beyond the Johnson radius (?)

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 (?)

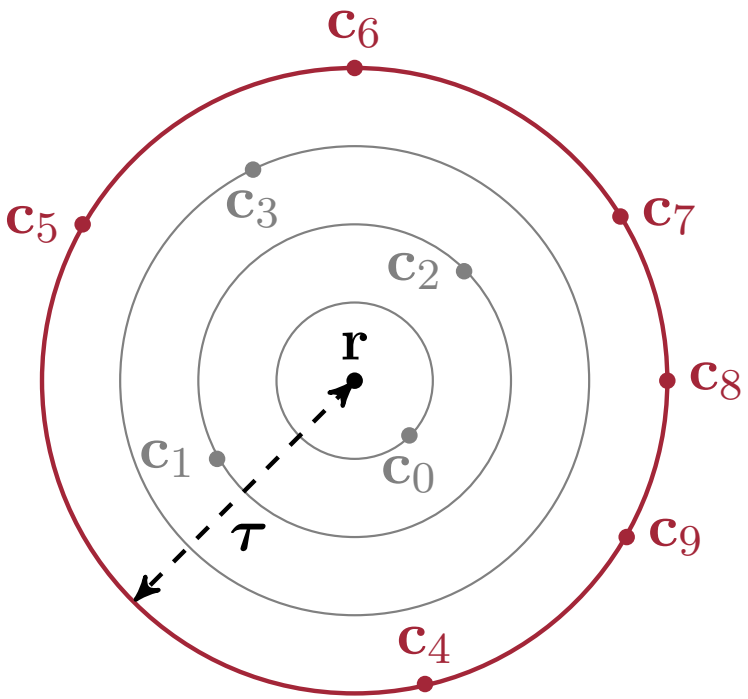
Outline

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:

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

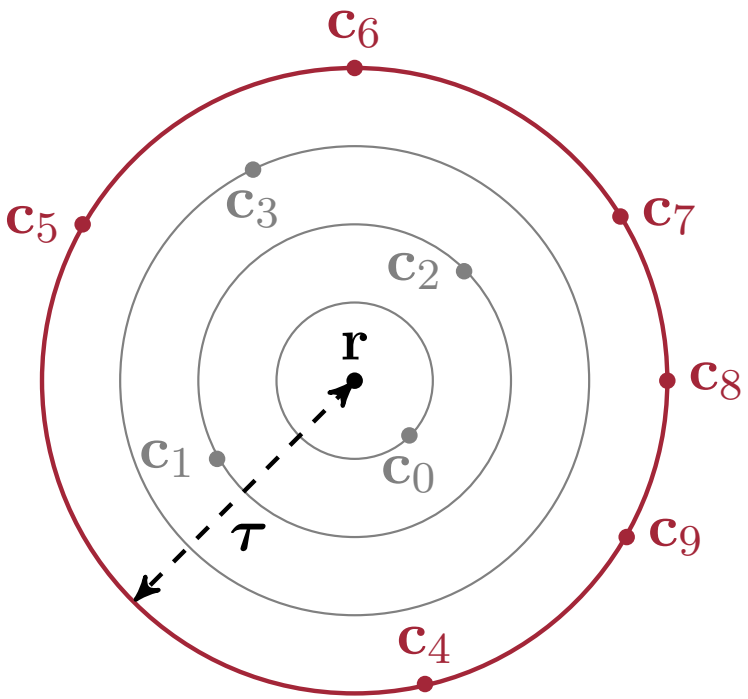


- Consider codewords $\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{\ell-1}$ in distance *exactly* τ
- Define $\overline{\mathcal{L}} = \{\mathbf{r} - \mathbf{c}_0, \ldots, \mathbf{r} - \mathbf{c}_{\ell-1}\}$
- $\mathrm{rk}(\mathbf{r}-\mathbf{c}_i-(\mathbf{r}-\mathbf{c}_j)) = \mathrm{rk}(\mathbf{c}_j-\mathbf{c}_i)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

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

Interpretation as Constant-Rank Code

decoding list:
$\mathcal{L} = \{\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{\ell-1}\} = \mathsf{C} \cap \mathcal{B}_\tau(\mathbf{r}) = \sum_{i=0}^{\tau} \left(\mathsf{C} \cap \mathcal{S}_i(\mathbf{r})\right)$

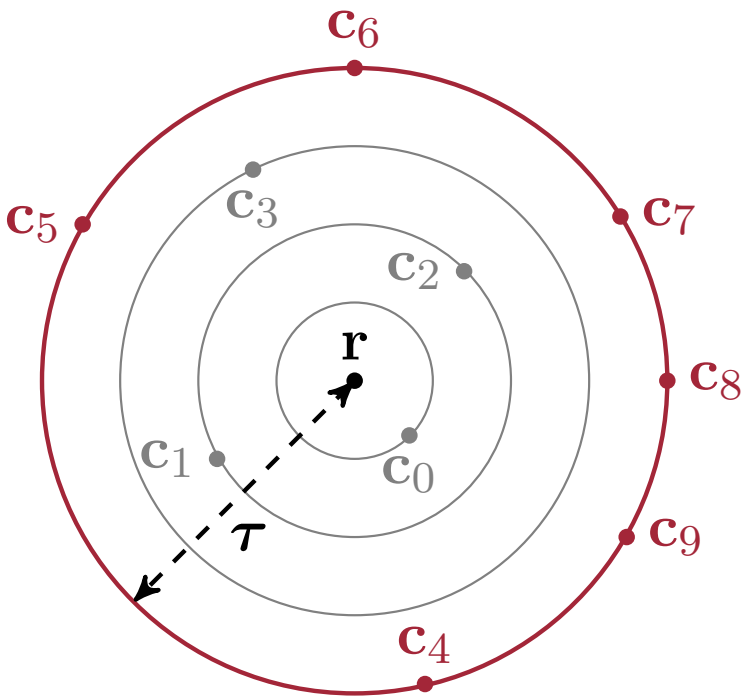


- Consider codewords $\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{\overline{\ell}-1}$ in distance *exactly* τ
- Define $\overline{\mathcal{L}} = \{\mathbf{r} - \mathbf{c}_0, \ldots, \mathbf{r} - \mathbf{c}_{\overline{\ell}-1}\}$
- $\mathrm{rk}(\mathbf{r}-\mathbf{c}_i-(\mathbf{r}-\mathbf{c}_j)) =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

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

Interpretation as Constant-Rank Code

decoding list:
$\mathcal{L} = \{\mathbf{c}_0, \mathbf{c}_1, \ldots, \mathbf{c}_{\ell-1}\} = \mathsf{C} \cap \mathcal{B}_\tau(\mathbf{r}) = \sum_{i=0}^{\tau} \left(\mathsf{C} \cap \mathcal{S}_i(\mathbf{r})\right)$



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

$\Longrightarrow$ 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*:*

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

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

- 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...

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*:*

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

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

- 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...

Upper Bound for Rank Metric Codes – Sketch of Proof

Sketch of Proof:

- $\mathsf{C} \cap \mathcal{S}_t(\mathbf{r}) = \{\mathbf{r} - \mathbf{c}_1, \ldots, \mathbf{r} - \mathbf{c}_{\overline{\ell}}\}$
  $\Longrightarrow$ 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:
  $\left|\mathsf{C} \cap \mathcal{S}_t(\mathbf{r})\right| \leq \mathsf{A}_{q^m}^R\left(n, d_R \geq d, t\right) \leq \mathsf{A}_{q^m}^R\left(n, d, t\right)$
- Use connection between constant-rank and constant-dimension codes from *Gadouleau & Yan (2010)*:
  $\mathsf{A}_{q^m}^R\left(n, d, t\right) \leq \mathsf{A}_q^S\left(n, d_S = 2(d-t), t\right)$
- Use upper bound on cardinality of constant-dimension codes by *Wang, Xing, Safavi-Naini (2003)*:
  $\mathsf{A}_q^S\left(n, d_S = 2(d-t), t\right) \leq \frac{\begin{bmatrix} n \\ t-(d-t)+1 \end{bmatrix}}{\begin{bmatrix} t \\ t-(d-t)+1 \end{bmatrix}}$

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

Upper Bound for Rank Metric Codes – Sketch of Proof

Sketch of Proof:

- $\mathsf{C} \cap \mathcal{S}_t(\mathbf{r}) = \{\mathbf{r} - \mathbf{c}_1, \ldots, \mathbf{r} - \mathbf{c}_{\overline{\ell}}\}$
  $\Longrightarrow$ 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:
  $\left|\mathsf{C} \cap \mathcal{S}_t(\mathbf{r})\right| \leq \mathsf{A}^R_{q^m}\left(n, d_R \geq d, t\right) \leq \mathsf{A}^R_{q^m}\left(n, d, t\right)$
- Use connection between constant-rank and constant-dimension codes from *Gadouleau & Yan (2010)*:
  $\mathsf{A}^R_{q^m}\left(n, d, t\right) \leq \mathsf{A}^S_q\left(n, d_S = 2(d-t), t\right)$
- Use upper bound on cardinality of constant-dimension codes by *Wang, Xing, Safavi-Naini (2003)*:
  $\mathsf{A}^S_q\left(n, d_S = 2(d-t), t\right) \leq \frac{\begin{bmatrix} n \\ t-(d-t)+1 \end{bmatrix}}{\begin{bmatrix} t \\ t-(d-t)+1 \end{bmatrix}}$

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

Upper Bound for Rank Metric Codes – Sketch of Proof

Sketch of Proof:

- $\mathsf{C} \cap \mathcal{S}_t(\mathbf{r}) = \{\mathbf{r} - \mathbf{c}_1, \ldots, \mathbf{r} - \mathbf{c}_{\overline{\ell}}\}$
  $\Longrightarrow$ 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:
  $\left|\mathsf{C} \cap \mathcal{S}_t(\mathbf{r})\right| \leq \mathsf{A}^R_{q^m}(n, d_R \geq d, t) \leq \mathsf{A}^R_{q^m}(n, d, t)$
- Use connection between constant-rank and constant-dimension codes from *Gadouleau & Yan (2010)*:
  $\mathsf{A}^R_{q^m}(n, d, t) \leq \mathsf{A}^S_q(n, d_S = 2(d-t), t)$
- Use upper bound on cardinality of constant-dimension codes by *Wang, Xing, Safavi-Naini (2003)*:
  $\mathsf{A}^S_q(n, d_S = 2(d-t), t) \leq \frac{\begin{bmatrix} n \\ t-(d-t)+1 \end{bmatrix}}{\begin{bmatrix} t \\ t-(d-t)+1 \end{bmatrix}}$

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

Upper Bound for Rank Metric Codes – Sketch of Proof

Sketch of Proof:

- $\mathsf{C} \cap \mathcal{S}_t(\mathbf{r}) = \{\mathbf{r} - \mathbf{c}_1, \ldots, \mathbf{r} - \mathbf{c}_{\overline{\ell}}\}$
  $\Longrightarrow$ 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:
  $\left|\mathsf{C} \cap \mathcal{S}_t(\mathbf{r})\right| \leq \mathsf{A}^R_{q^m}\left(n, d_R \geq d, t\right) \leq \mathsf{A}^R_{q^m}\left(n, d, t\right)$
- Use connection between constant-rank and constant-dimension codes from *Gadouleau & Yan (2010)*:
  $\mathsf{A}^R_{q^m}\left(n, d, t\right) \leq \mathsf{A}^S_q\left(n, d_S = 2(d-t), t\right)$
- Use upper bound on cardinality of constant-dimension codes by *Wang, Xing, Safavi-Naini (2003)*:
  $\mathsf{A}^S_q\left(n, d_S = 2(d-t), t\right) \leq \frac{\begin{bmatrix} n \\ t-(d-t)+1 \end{bmatrix}}{\begin{bmatrix} t \\ t-(d-t)+1 \end{bmatrix}}$

Summing up for $t = \lfloor (d-1)/2 \rfloor + 1, \ldots, \tau$ 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* C *over* $\mathbb{F}_{q^m}$ *and a word* $\mathbf{r} \in \mathbb{F}_{q^m}^n$ *such that*

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

- There exists a rank-metric code such that max. list size is **exponential** in n for $\tau > \lfloor (d-1)/2 \rfloor$.
  $\Longrightarrow$ 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*

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

- There exists a rank-metric code such that max. list size is **exponential** in n for $\tau > \lfloor (d-1)/2 \rfloor$.
  $\Longrightarrow$ 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*

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

- There exists a rank-metric code such that max. list size is **exponential** in n for $\tau > \lfloor (d-1)/2 \rfloor$.
  $\Longrightarrow$ 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 $\mathbf{r} = \mathbf{0}$:
  - $\mathrm{rk}(\mathbf{r} - \mathbf{a}_i) = \mathrm{rk}(\mathbf{a}_i) = \tau$ for all i (constant-rank code)
  - $d_R(\mathbf{a}_i, \mathbf{a}_j) = \mathrm{rk}(\mathbf{a}_i - \mathbf{a}_j) \geq d$

  $\Rightarrow \mathbf{a}_0, \mathbf{a}_1, \dots$ 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. $\ell \geq |\mathsf{C} \cap \mathcal{S}_\tau(\mathbf{r})| = |\mathsf{CR}| = q^{(n-\tau)(\tau-\lfloor(d-1)/2\rfloor)}$. □

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

  $\Rightarrow \mathbf{a}_0, \mathbf{a}_1, \dots$ 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. $\ell \geq |\mathsf{C} \cap \mathcal{S}_\tau(\mathbf{r})| = |\mathsf{CR}| = q^{(n-\tau)(\tau-\lfloor(d-1)/2\rfloor)}$. □

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

  $\Rightarrow \mathbf{a}_0, \mathbf{a}_1, \dots$ 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. $\ell \geq |\mathsf{C} \cap \mathcal{S}_\tau(\mathbf{r})| = |\mathsf{CR}| = q^{(n-\tau)(\tau-\lfloor(d-1)/2\rfloor)}$. □

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 $q^{(n-\tau)(\tau-\lfloor(d-1)/2\rfloor)}$

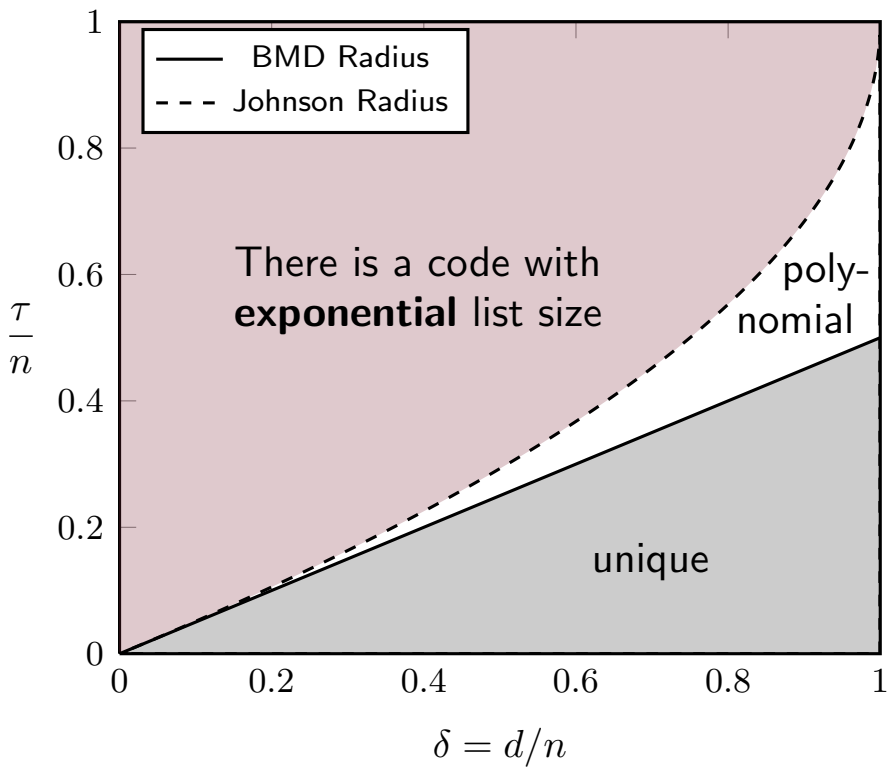
  Denote the codewords of this constant-rank code by $\{\mathbf{a}_0, \mathbf{a}_1, \dots\}$.
- Choose $\mathbf{r} = \mathbf{0}$:
  - $\mathrm{rk}(\mathbf{r} - \mathbf{a}_i) = \mathrm{rk}(\mathbf{a}_i) = \tau$ for all i (constant-rank code)
  - $d_R(\mathbf{a}_i, \mathbf{a}_j) = \mathrm{rk}(\mathbf{a}_i - \mathbf{a}_j) \geq d$

  $\Rightarrow \mathbf{a}_0, \mathbf{a}_1, \dots$ are codewords of a code with rank distance at least d
  $\Rightarrow$ and lie all on a sphere of radius τ around $\mathbf{r}$

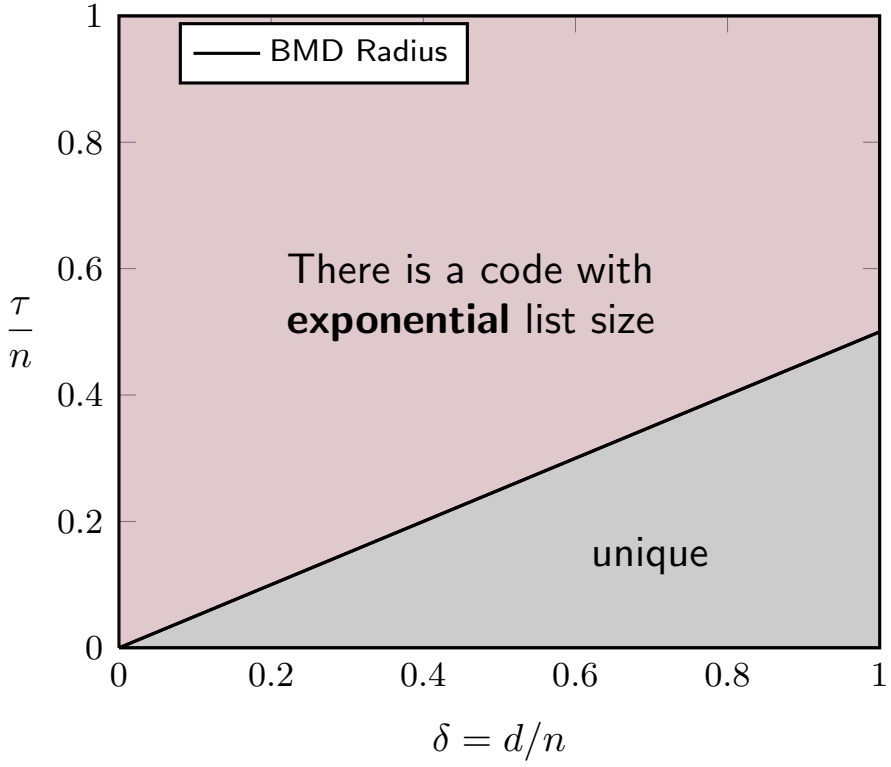
There exists an $(n, M, d_R \geq d)_R$ code C of min. rank distance at least d s.t. $\ell \geq |\mathsf{C} \cap \mathcal{S}_\tau(\mathbf{r})| = |\mathsf{CR}| = q^{(n-\tau)(\tau-\lfloor(d-1)/2\rfloor)}$. □

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* C *over* $\mathbb{F}_{q^m}$ *and a word* $\mathbf{r} \in \mathbb{F}_{q^m}^n$ *such that*

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

$\Longrightarrow$ This lower bound is asymptotically tight!

Outline

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!