Bounds on List Decoding of Rank Metric Codes

Antonia Wachter-Zeh

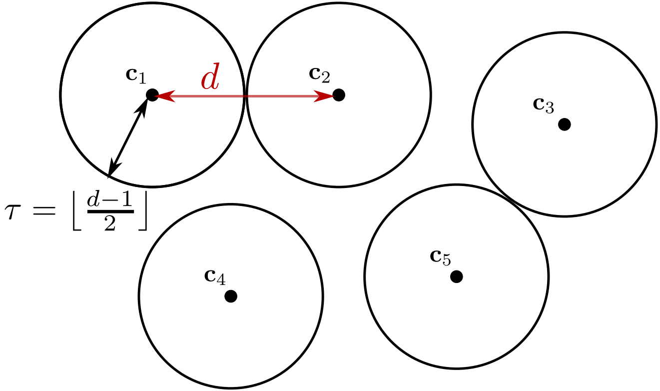
Institute of Communications Engineering, Ulm University, Ulm, Germany and
Institut de Recherche Mathématique de Rennes (IRMAR),
Université de Rennes 1, Rennes, France

October 8, 2012

Journées Codage et Cryptographie 2012

Motivation — Reed–Solomon vs. Gabidulin Codes

For a code $\mathcal{C}$ of length n, dimension k and minimum distance d, unique decoding is possible up to $\tau = \left\lfloor \frac{d-1}{2} \right\rfloor$.



What about decoding algorithms for Gabidulin codes?
Similar to Reed–Solomon codes?

Reed–Solomon vs. Gabidulin Codes — Algorithms

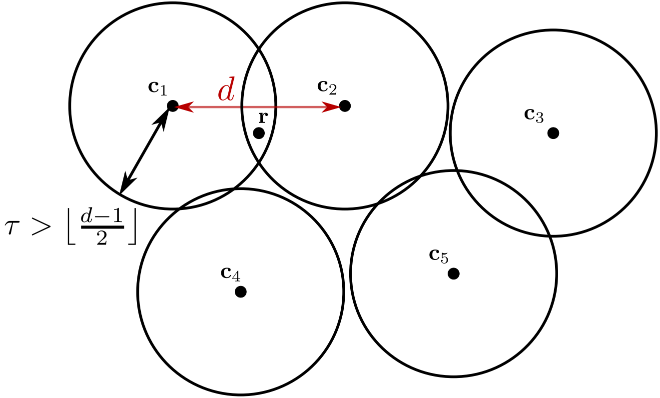
Decoding up to half the minimum distance $\tau = \left\lfloor \frac{d-1}{2} \right\rfloor$

	Reed–Solomon Codes	Gabidulin Codes
System of equations	Peterson, . . .	Gabidulin
Shift–Register Synthesis	Berlekamp–Massey	Paramonov–Tretjakov, Richter–Plass
Euclidean Algorithm	Sugiyama, . . .	Gabidulin
Interpolation	Welch–Berlekamp	Loidreau
⋮	⋮	⋮

Many parallels between Reed–Solomon and Gabidulin codes!

List Decoding

For a code $\mathcal{C}$ of length n, dimension k and minimum distance d, there can be several codewords in a ball of radius $\tau > \left\lfloor \frac{d-1}{2} \right\rfloor$.



What about decoding algorithms for Gabidulin codes?
Similar to Reed–Solomon codes?

Reed–Solomon vs. Gabidulin Codes — Algorithms

Decoding beyond half the minimum distance $\tau > \left\lfloor \frac{d-1}{2} \right\rfloor$

	Reed–Solomon Codes	Gabidulin Codes
Interpolation (List Decoding)	Sudan Guruswami–Sudan (and many accelerations)	?
Syndrome-based (Unique Decoding)	Schmidt–Sidorenko	

Is polynomial–time list decoding possible for Gabidulin codes?

Outline

Outline

Rank Metric

Rank Metric

- Let $\mathcal{B}$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ where q is a power of a prime
- Each vector $\mathbf{x} \in \mathbb{F}_{q^m}^n$ can be mapped on a matrix $\mathbf{X} \in \mathbb{F}_q^{m \times n}$
- Rank norm: $\mathrm{rank}(\mathbf{x}) \overset{\mathrm{def}}{=}$ rank of $\mathbf{X}$ over $\mathbb{F}_q$

Minimum Rank Distance of a block code $\mathcal{C}$:

- $d \overset{\mathrm{def}}{=} \min\{\mathrm{rank}(\mathbf{c}_1 - \mathbf{c}_2) \mid \mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}, \mathbf{c}_1 \neq \mathbf{c}_2\} \leq n - k + 1$
- Codes with $d = n - k + 1$ are called Maximum Rank Distance (MRD) codes

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

- $f(x) \overset{\mathrm{def}}{=} \sum_{i=0}^{d_f} f_i x^{[i]} = \sum_{i=0}^{d_f} f_i x^{q^i}$ with $f_i \in \mathbb{F}_{q^m}$.
- If $f_{d_f} \neq 0$, define the q-degree: $\deg_q f(x) = d_f$.

Rank Metric

Rank Metric

- Let $\mathcal{B}$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ where q is a power of a prime
- Each vector $\mathbf{x} \in \mathbb{F}_{q^m}^n$ can be mapped on a matrix $\mathbf{X} \in \mathbb{F}_q^{m \times n}$
- Rank norm: $\mathrm{rank}(\mathbf{x}) \stackrel{\text{def}}{=}$ rank of $\mathbf{X}$ over $\mathbb{F}_q$

Minimum Rank Distance of a block code $\mathcal{C}$:

- $d \stackrel{\text{def}}{=} \min\{\mathrm{rank}(\mathbf{c}_1 - \mathbf{c}_2) \mid \mathbf{c}_1, \mathbf{c}_2 \in \mathcal{C}, \mathbf{c}_1 \neq \mathbf{c}_2\} \leq n - k + 1$
- Codes with $d = n - k + 1$ are called Maximum Rank Distance (MRD) codes

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 $f_i \in \mathbb{F}_{q^m}$.
- If $f_{d_f} \neq 0$, define the q-degree: $\deg_q f(x) = d_f$.

Gabidulin Codes

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

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

$$\mathcal{G}(n,k) \overset{\text{def}}{=} \left\{ \mathbf{c} = (f(\alpha_0)\ f(\alpha_1)\ \ldots\ f(\alpha_{n-1})) \,\middle|\, \deg_q f(x) < k \right\},$$

  where all $f(x)$ are linearized polynomials and $\alpha_0, \ldots, \alpha_{n-1} \in \mathbb{F}_{q^m}$ are linearly independent over $\mathbb{F}_q$.

Minimum Rank Distance of a Gabidulin Code

- $d = \min\{\mathrm{rank}(\mathbf{c}) \mid \mathbf{c} \in \mathcal{G}, \mathbf{c} \neq \mathbf{0}\} = n - k + 1.$

Outline

Problem Statement

Is polynomial–time list decoding possible for rank metric codes (and in particular for Gabidulin codes)?

Problem (Maximum List Size)

Let $\mathcal{C}(n, M, d)$ be a code over $\mathbb{F}_{q^m}$ with $n \leq m$ and minimum rank distance d. Let $\tau < d$. Find a lower and upper bound on the maximum number of codewords ℓ in a ball of rank radius τ. Hence, find a bound on

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

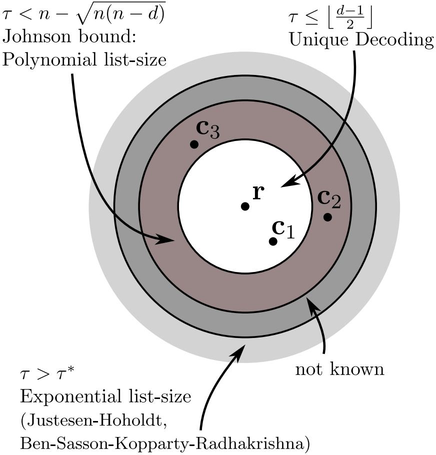
Interpretation:

- Lower exponential bound: no polynomial-time list decoding,
- Upper polynomial bound: polynomial-time list decoding might exist.

Outline

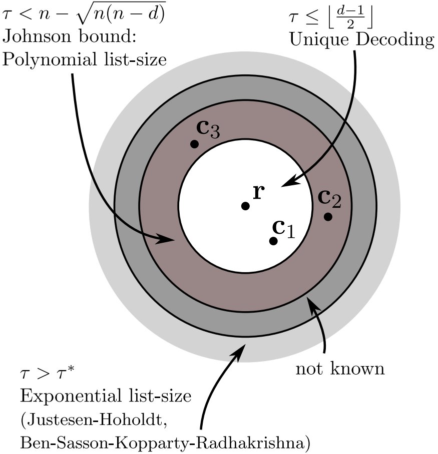
Bounds on the Maximal List-Size

Reed–Solomon codes

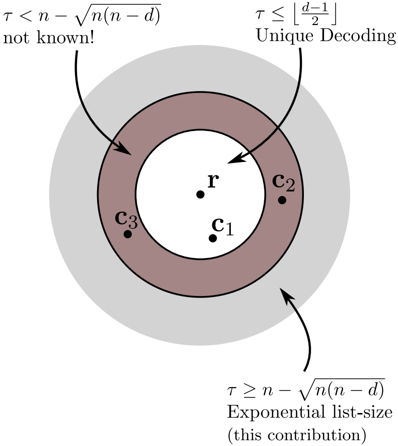


Bounds on the Maximal List-Size

Reed–Solomon codes



Gabidulin codes



A Lower Bound on the List Size

Theorem (Lower Bound on the List Size)

Let the Gabidulin code $\mathcal{G}(n,k)$ over $\mathbb{F}_{q^m}$ with $n \leq m$ and $d = n-k+1$ be given and let $\tau < d$. Then, there exists a word $\mathbf{r} \in \mathbb{F}_{q^m}^n$ such that

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

and for the special case of $n = m$: $\ell \geq q^n q^{2n\tau-\tau^2-nd}$.

- For $n = m$ this is $\ell \geq q^{n(1-\epsilon)} \cdot q^{2n\tau-\tau^2-nd+n\epsilon}$
- Exponential in n if $\tau \geq n - \sqrt{n(n-d+\epsilon)}$ and $0 \leq \epsilon < 1$ (= Johnson radius).
- Proof similar to the proof of Justesen-Hoholdt for RS codes.

A Lower Bound on the List Size

Theorem (Lower Bound on the List Size)

Let the Gabidulin code $\mathcal{G}(n,k)$ *over* $\mathbb{F}_{q^m}$ *with* $n \leq m$ *and* $d = n-k+1$ *be given and let* $\tau < d$*. Then, there exists a word* $\mathbf{r} \in \mathbb{F}_{q^m}^n$ *such that*

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

and for the special case of $n = m$: $\ell \geq q^n q^{2n\tau-\tau^2-nd}$.

- For $n = m$ this is $\ell \geq q^{n(1-\epsilon)} \cdot q^{2n\tau-\tau^2-nd+n\epsilon}$
- Exponential in n if $\tau \geq n - \sqrt{n(n-d+\epsilon)}$ and $0 \leq \epsilon < 1$ ($=$ Johnson radius).
- Proof similar to the proof of Justesen-Hoholdt for RS codes.

A Lower Bound on the List Size – Proof

Proof (i)

- $\mathcal{P}^* \stackrel{\text{def}}{=}$ set of all monic linearized polynomials of $\deg_q = n - \tau$ and a root space over $\mathbb{F}_{q^n}$ of dimension $n - \tau > k - 1$
- $|\mathcal{P}^*| = \begin{bmatrix} n \\ n-\tau \end{bmatrix}$
- $\mathcal{P} \stackrel{\text{def}}{=}$ subset of $\mathcal{P}^*$ such that all q-monomials of q-degree greater than or equal to k have the same coefficients
- There are $(q^m)^{n-\tau-k}$ possibilities to choose the highest $n - \tau - (k-1)$ coefficients
- There exist coefficients such that $|\mathcal{P}| \geq \frac{\begin{bmatrix} n \\ n-\tau \end{bmatrix}}{(q^m)^{n-\tau-k}}$
- For any $f(x), g(x) \in \mathcal{P}$, $\deg_q(f(x) - g(x)) < k$, is evaluation polynomial of a codeword of $\mathcal{G}(n, k)$

. . .

A Lower Bound on the List Size – Proof

Proof (ii)

- Let $f(x), g(x) \in \mathcal{P}$
- Let $\mathcal{A} = \{\alpha_0, \alpha_1, \dots, \alpha_{n-1}\}$ be a basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$
- Let $\mathbf{r} = (r_0 \; r_1 \; \dots \; r_{n-1}) = (f(\alpha_0) \; f(\alpha_1) \; \dots \; f(\alpha_{n-1}))$
- Let $\mathbf{c}$ be the evaluation of $f(x) - g(x)$ at $\mathcal{A}$
- Then, $\mathbf{r} - \mathbf{c}$ is the evaluation of $f(x) - f(x) + g(x) = g(x) \in \mathcal{P}$, whose root space has dimension $n - \tau$ and all roots are in $\mathbb{F}_{q^n}$
- $\dim \ker(\mathbf{r} - \mathbf{c}) = n - \tau$ and $\mathrm{rk}(\mathbf{r} - \mathbf{c}) = \tau$

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

$$\Longrightarrow \boldsymbol{\ell} \geq |\boldsymbol{\mathcal{P}}| \geq \frac{\begin{bmatrix} \boldsymbol{n} \\ \boldsymbol{n-\tau} \end{bmatrix}}{(\boldsymbol{q^m})^{\boldsymbol{n-\tau-k}}}. \qquad \square$$

Outline

An Upper Bound on the List Size

Theorem (Upper Bound on the List Size)

Let **any** *rank metric code* $\mathcal{C}(n, M, d)$ *over* $\mathbb{F}_{q^m}$ *with* $n \leq m$ *and minimum rank distance* d *be given. Let* $\tau < d$. *Then, for* **any** *word* $\mathbf{r} \in \mathbb{F}_{q^m}^n$ *and hence, for the maximum list size, the following holds*

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

$$\leq 4 \sum_{t=\left\lfloor \frac{d-1}{2} \right\rfloor + 1}^{\tau} q^{(2t-d+1)(n-t)}.$$

- 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 up to the Johnson bound.

A Lower Bound on the List Size

Theorem (Lower Bound on the List-Size)

Let $n \leq m$, $\tau \geq \lfloor (d-1)/2 \rfloor + 1$ *and* $\tau \leq n - \tau$.
Then, there exists a rank metric code $\mathcal{C}(n, M, d_R \geq d)$ *over* $\mathbb{F}_{q^m}$ *of length* n *and minimum rank distance* $d_R \geq d$, *and a word* $\mathbf{r} \in \mathbb{F}_{q^m}^n$ *such that*

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

- Shows there exists a rank metric code and a received word such that list size is **exponential** in n for $\tau > \lfloor (d-1)/2 \rfloor$.
  $\Rightarrow$ No polynomial-time list decoding for these codes!
- $\mathcal{C}(n, M, d_R \geq d)$ might be non-linear and non-MRD.
- The restriction $\tau \leq n - \tau$ is always fulfilled for $\tau = \lfloor (d-1)/2 \rfloor + 1$ and $k > 1$.
- Proof uses interpretation of $\{\mathbf{r} - \mathbf{c}_1, \mathbf{r} - \mathbf{c}_2, \dots, \mathbf{r} - \mathbf{c}_\ell\}$ as constant-rank code of rank τ and minimum rank distance d.

A Lower Bound on the List Size

Theorem (Lower Bound on the List-Size)

Let $n \leq m$, $\tau \geq \lfloor (d-1)/2 \rfloor + 1$ and $\tau \leq n - \tau$.
Then, there exists a rank metric code $\mathcal{C}(n, M, d_R \geq d)$ over $\mathbb{F}_{q^m}$ of length n and minimum rank distance $d_R \geq d$, and a word $\mathbf{r} \in \mathbb{F}_{q^m}^n$ such that

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

- Shows there exists a rank metric code and a received word such that list size is **exponential** in n for $\tau > \lfloor (d-1)/2 \rfloor$.
  $\Rightarrow$ No polynomial-time list decoding for these codes!
- $\mathcal{C}(n, M, d_R \geq d)$ might be non-linear and non-MRD.
- The restriction $\tau \leq n - \tau$ is always fulfilled for $\tau = \lfloor (d-1)/2 \rfloor + 1$ and $k > 1$.
- Proof uses interpretation of $\{\mathbf{r} - \mathbf{c}_1, \mathbf{r} - \mathbf{c}_2, \dots, \mathbf{r} - \mathbf{c}_\ell\}$ as constant-rank code of rank τ and minimum rank distance d.

A Lower Bound on the List Size

Theorem (Lower Bound on the List-Size)

Let $n \leq m$, $\tau \geq \lfloor (d-1)/2 \rfloor + 1$ and $\tau \leq n - \tau$.
Then, there exists a rank metric code $\mathcal{C}(n, M, d_R \geq d)$ over $\mathbb{F}_{q^m}$ of length n and minimum rank distance $d_R \geq d$, and a word $\mathbf{r} \in \mathbb{F}_{q^m}^n$ such that

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

- Shows there exists a rank metric code and a received word such that list size is **exponential** in n for $\tau > \lfloor (d-1)/2 \rfloor$.
  $\Rightarrow$ No polynomial-time list decoding for these codes!
- $\mathcal{C}(n, M, d_R \geq d)$ might be non-linear and non-MRD.
- The restriction $\tau \leq n - \tau$ is always fulfilled for $\tau = \lfloor (d-1)/2 \rfloor + 1$ and $k > 1$.
- Proof uses interpretation of $\{\mathbf{r} - \mathbf{c}_1, \mathbf{r} - \mathbf{c}_2, \dots, \mathbf{r} - \mathbf{c}_\ell\}$ as constant-rank code of rank τ and minimum rank distance d.

Outline

Conclusion

We have shown three bounds on the list size of rank metric codes:

The lower bound for **Gabidulin codes**

- is based on the evaluation of linearized polynomials,
- shows that polynomial-time list decoding is not possible for $\tau \geq n - \sqrt{n(n-d+\epsilon)}$.

The upper bound for **any** rank metric code

- uses subspace properties,
- is exponential in n.

The lower bound for rank metric codes

- uses the interpretation as constant-rank code,
- **shows that there exists a rank metric code with exponential list size for $\tau \geq \lfloor (d-1)/2 \rfloor + 1$.**

Conclusion

We have shown three bounds on the list size of rank metric codes:

The lower bound for **Gabidulin codes**

- is based on the evaluation of linearized polynomials,
- shows that polynomial-time list decoding is not possible for $\tau \geq n - \sqrt{n(n-d+\epsilon)}$.

The upper bound for **any** rank metric code

- uses subspace properties,
- is exponential in n.

The lower bound for rank metric codes

- uses the interpretation as constant-rank code,
- **shows that there exists a rank metric code with exponential list size for $\tau \geq \lfloor (d-1)/2 \rfloor + 1$.**

Conclusion

We have shown three bounds on the list size of rank metric codes:

The lower bound for **Gabidulin codes**

- is based on the evaluation of linearized polynomials,
- shows that polynomial-time list decoding is not possible for $\tau \geq n - \sqrt{n(n-d+\epsilon)}$.

The upper bound for **any** rank metric code

- uses subspace properties,
- is exponential in n.

The lower bound for rank metric codes

- uses the interpretation as constant-rank code,
- **shows that there exists a rank metric code with exponential list size for $\boldsymbol{\tau \geq \lfloor (d-1)/2 \rfloor + 1}$.**

Merci pour votre attention !