Higher Degrees Symmetric Rank Metric Codes

ALCOCRYPT 2023

Alessandro Neri

22 February 2023

Joint work with Arthur Bik

Contents

Prologue
(Symmetric) Rank Metric Codes

Coding Theory

- Field $\mathbb{F}$. $\mathbb{F} = \mathbb{F}_q$
- V finite dimensional $\mathbb{F}$-vector space.
- $\mathrm{wt} : V \to \mathbb{N}$ **weight function**.
- $\delta : V \times V \to \mathbb{R}_{\geq 0}$; $\delta(u, v) := \mathrm{wt}(u - v)$ **distance** function.
- (V, δ) **metric space**.

Coding Theory

- Field $\mathbb{F}$. $\mathbb{F} = \mathbb{F}_q$
- V finite dimensional $\mathbb{F}$-vector space.
- $\mathrm{wt} : V \to \mathbb{N}$ **weight function**.
- $\delta : V \times V \to \mathbb{R}_{\geq 0}$; $\delta(u, v) := \mathrm{wt}(u - v)$ **distance** function.
- (V, δ) **metric space**.

A $[V, k, d]$ **code** $\mathcal{C}$ is a k-dimensional $\mathbb{F}$-subspace of V endowed with the metric δ. The parameter d is known as the **minimum distance** of $\mathcal{C}$, that is

$$\begin{aligned} d &= \min\{\delta(u, v) \ : \ u, v \in \mathcal{C}, u \neq v.\} \\ &= \min\{\mathrm{wt}(u) \ : \ u \in \mathcal{C} \setminus \{0\}\} \end{aligned}$$

Rank Metric Codes

1. Rank metric codes
   - $V = \mathbb{F}^{n\times m}$.
   - $\mathrm{wt} = \mathrm{rk}$ is the **rank weight** on $\mathbb{F}^{n\times m}$.
   - $\delta = \mathrm{d}_{\mathrm{rk}}$ the **rank distance** on $\mathbb{F}^{n\times m}$ defined as

$$\mathrm{d}_{\mathrm{rk}}(A, B) := \mathrm{rk}(A - B).$$

Rank Metric Codes

1. Rank metric codes
   - $V = \mathbb{F}^{n\times m}$.
   - $\mathrm{wt} = \mathrm{rk}$ is the **rank weight** on $\mathbb{F}^{n\times m}$.
   - $\delta = \mathrm{d}_{\mathrm{rk}}$ the **rank distance** on $\mathbb{F}^{n\times m}$ defined as

$$\mathrm{d}_{\mathrm{rk}}(A, B) := \mathrm{rk}(A - B).$$

- Introduced by **Delsarte** for combinatorial interest via association schemes (over finite fields). (1978)
- Reintroduced independently by **Gabidulin** (over finite fields). (1985)
- Reintroduced by **Roth** (over any field) for applications in criss-cross error correction. (1991)
- Renovated interest due to **Kötter–Kschischang–Silva** for their application in linear network coding. (2008)

Rank Metric Codes with Restrictions

Rank metric codes with **restrictions**

- Delsarte–Goethals analyzed **skew-symmetric rank metric codes** (1975)
- Later also Coopersmith did the same (1998)
- de Boer instead focused on **symmetric rank metric codes** in connection with linear codes (1996)
- Gabidulin and Pilipchuk: **decoding** of symmetric errors in rank metric codes beyond half the minimum distance (2004–2006)
- Schmidt **improved** the existing **bounds** for symmetric rank metric codes via association schemes (2010–2015)
- Additional works on **symmetric** and **Hermitian rank metric codes**: Schmidt (2018–2020) Longobardi–Lunardon–Trombetti–Zhou (2020), Zhou (2020), Trombetti–Zullo (2021), De La Cruz–Evilla–Ozbudak (2021) Couvreur (2022), ...

Symmetric Rank Metric Codes

$$\mathrm{Sym}_n(\mathbb{F}) = \{A \in \mathbb{F}^{n\times n} \,:\, A^\top = A\}.$$

Symmetric Rank Metric Codes

$$\mathrm{Sym}_n(\mathbb{F}) = \{A \in \mathbb{F}^{n\times n} \,:\, A^\top = A\}.$$

Definition

A **symmetric rank metric code** $\mathcal{C}$ is an $\mathbb{F}$-subspace of $\mathrm{Sym}_n(\mathbb{F})$ equipped with the rank distance. The **minimum rank distance** of $\mathcal{C}$ is

$$\mathsf{d}_{\mathsf{rk}}(\mathcal{C}) = \min\{\mathsf{rk}(A) \,:\, A \in \mathcal{C} \setminus \{0\}\}.$$

Symmetric Rank Metric Codes

$$\mathrm{Sym}_n(\mathbb{F}) = \{A \in \mathbb{F}^{n\times n} \,:\, A^\top = A\}.$$

Definition

A **symmetric rank metric code** $\mathcal{C}$ is an $\mathbb{F}$-subspace of $\mathrm{Sym}_n(\mathbb{F})$ equipped with the rank distance. The **minimum rank distance** of $\mathcal{C}$ is

$$\mathsf{d}_{\mathsf{rk}}(\mathcal{C}) = \min\{\mathsf{rk}(A) \,:\, A \in \mathcal{C} \setminus \{0\}\}.$$

- **Singleton-like bound** (Schmidt 2015): **only for $\mathbb{F} = \mathbb{F}_q$**

$$\dim_{\mathbb{F}}(\mathcal{C}) \leq \begin{cases} \frac{n(n-\mathsf{d}_{\mathsf{rk}}(\mathcal{C})+2)}{2} & \text{if } n-\mathsf{d}_{\mathsf{rk}}(\mathcal{C}) \text{ is even} \\ \frac{(n+1)(n-\mathsf{d}_{\mathsf{rk}}(\mathcal{C})+1)}{2} & \text{if } n-\mathsf{d}_{\mathsf{rk}}(\mathcal{C}) \text{ is odd} \end{cases}$$

- The bound is tight. Constructions over **any field** admitting degree n cyclic Galois extension: **symmetric Gabidulin codes** (de Boer 1996)

Symmetric Matrices as Homogeneous Polynomials

$$f = \sum_{1 \leq i \leq j \leq n} a_{i,j} x_i x_j \in \mathbb{F}[x_1, \ldots, x_n]_2$$

We can associate the matrix

$$C_f = \begin{pmatrix} 2a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{1,2} & 2a_{2,2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_{n-1,n} \\ a_{1,n} & \cdots & a_{n-1,n} & 2a_{n,n} \end{pmatrix}.$$

Symmetric Matrices as Homogeneous Polynomials

$$f = \sum_{1 \le i \le j \le n} a_{i,j} x_i x_j \in \mathbb{F}[x_1, \ldots, x_n]_2$$

We can associate the matrix

$$C_f = \begin{pmatrix} 2a_{1,1} & a_{1,2} & \cdots & a_{1,n} \\ a_{1,2} & 2a_{2,2} & \ddots & \vdots \\ \vdots & \ddots & \ddots & a_{n-1,n} \\ a_{1,n} & \cdots & a_{n-1,n} & 2a_{n,n} \end{pmatrix}.$$

Proposition

If $\mathbf{char}(\mathbb{F}) \neq 2$ then **(*)**

$$\mathsf{rk}(C_f) = \mathsf{min}\{r \mid f = g(\ell_1, \ldots, \ell_r), \ell_1, \ldots, \ell_r \in \mathbb{F}[x_1, \ldots, x_n]_1\}.$$

Generalizing to degree $d \geq 2$

Symmetric matrices of order n are **homogeneous polynomials of degree 2** in n variables.

Generalizing to degree $d \geq 2$

Symmetric matrices of order n are **homogeneous polynomials of degree 2** in n variables.

- Let us investigate how to generalize the study of **symmetric matrices to higher degree** $d \geq 2$.
- We focus on the space of homogeneous degree d polynomials $\mathbb{F}[x_1, \ldots, x_n]_d$.

Generalizing to degree $d \geq 2$

Symmetric matrices of order n are **homogeneous polynomials of degree 2** in n variables.

- Let us investigate how to generalize the study of **symmetric matrices to higher degree** $d \geq 2$.
- We focus on the space of homogeneous degree d polynomials $\mathbb{F}[x_1, \ldots, x_n]_d$.
- Which metric can we consider on $\mathbb{F}[x_1, \ldots, x_n]_d$?
- Homogeneous degree d polynomials are naturally d-way symmetric tensors.

Generalizing to degree $d \geq 2$

Symmetric matrices of order n are **homogeneous polynomials of degree 2** in n variables.

- Let us investigate how to generalize the study of **symmetric matrices to higher degree** $d \geq 2$.
- We focus on the space of homogeneous degree d polynomials $\mathbb{F}[x_1, \ldots, x_n]_d$.
- Which metric can we consider on $\mathbb{F}[x_1, \ldots, x_n]_d$?
- Homogeneous degree d polynomials are naturally d-way symmetric tensors.
- There are several **equivalent** ways to characterize rank of (symmetric) matrices,
- Generalizing them to d-tensors yields to several **different** notions.

Part 1
Higher Degrees Homogeneous Polynomials and Essential Rank Metric Codes

- **Essential rank** of degree d polynomials.
- Well-defined notion of **Space of essential variables**.
- Notion of **Catalecticant matrix** associated to a polynomial
- How these three objects are related.
- They turn out to be rank metric codes with special symmetries!.

Essential Rank for Degree d Polynomials

The **essential rank** of a degree-d polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]_d$ can be defined as a natural generalization of **(*)** and is given by

$$\mathrm{ess}(f) = \min\{r \mid f = g(\ell_1, \ldots, \ell_r), \ell_1, \ldots, \ell_r \in \mathbb{F}[x_1, \ldots, x_n]_1\}$$

Remark

The essential rank of a polynomial is equal to the **minimum number of variables** that are needed in order to represent it, up to linear changes of variables.

Essential Rank for Degree d Polynomials

The **essential rank** of a degree-d polynomial $f \in \mathbb{F}[x_1, \ldots, x_n]_d$ can be defined as a natural generalization of **(*)** and is given by

$$\mathrm{ess}(f) = \min\{r \mid f = g(\ell_1, \ldots, \ell_r), \ell_1, \ldots, \ell_r \in \mathbb{F}[x_1, \ldots, x_n]_1\}$$

Remark

The essential rank of a polynomial is equal to the **minimum number of variables** that are needed in order to represent it, up to linear changes of variables.

- $\mathrm{ess} : \mathbb{F}[x_1, \ldots, x_n]_d \longrightarrow \mathbb{N}$ is a weight
- It induces a metric: $\mathrm{d_{ess}} : \mathbb{F}[x_1, \ldots, x_n]_d \times \mathbb{F}[x_1, \ldots, x_n]_d \longrightarrow \mathbb{R}_{\geq 0}$.
- We can define **essential rank metric codes**.

Space of Essential Variables

Let $f \in S_{n,d}(\mathbb{F})$ be such that $\mathsf{ess}(f) = r$ and let $f = g(\ell_1, \ldots, \ell_r)$.

- $\ell_1, \ldots, \ell_r$ are **not** unique.

Space of Essential Variables

Let $f \in S_{n,d}(\mathbb{F})$ be such that $\mathsf{ess}(f) = r$ and let $f = g(\ell_1, \ldots, \ell_r)$.

- $\ell_1, \ldots, \ell_r$ are **not** unique.
- $\langle \ell_1, \ldots, \ell_r \rangle_{\mathbb{F}}$ is unique

Space of Essential Variables

Let $f \in S_{n,d}(\mathbb{F})$ be such that $\mathsf{ess}(f) = r$ and let $f = g(\ell_1, \ldots, \ell_r)$.

- $\ell_1, \ldots, \ell_r$ are **not** unique.
- $\langle \ell_1, \ldots, \ell_r \rangle_{\mathbb{F}}$ is unique

Definition

The **space of essential variables** of f is

$$V_{\mathsf{ess}}(f) = \langle \ell_1, \ldots, \ell_r \rangle_{\mathbb{F}}$$

N.B. $\mathsf{ess}(f) = \dim_{\mathbb{F}}(V_{\mathsf{ess}}(f))$

Example

$$f = 3x_1^3 + 8x_1^2x_2 + 5x_1^2x_3 + 12x_1x_2^2 + 4x_1x_2x_3 + 4x_1x_3^2 + 8x_2^3 + 2x_2x_3^2 + x_3^3.$$

Question

How to compute its essential rank?

Example

$$f = 3x_1^3 + 8x_1^2x_2 + 5x_1^2x_3 + 12x_1x_2^2 + 4x_1x_2x_3 + 4x_1x_3^2 + 8x_2^3 + 2x_2x_3^2 + x_3^3.$$

Question

How to compute its essential rank?

$$\begin{aligned} f &= (x_1 + 2x_2)(x_1 + x_3)^2 + (x_1 + 2x_2)^3 + (x_1 + x_3)^3 \\ &=: g(x_1 + 2x_2, x_1 + x_3). \end{aligned}$$

- $V_{\mathrm{ess}}(f) \subseteq \langle x_1 + 2x_2, x_1 + x_3 \rangle_{\mathbb{F}}$
- $\mathrm{ess}(f) \leq 2$.

Not an easy task ... **apparently**.

The Ring of Homogeneous Differentials

- $S_{n,d}(\mathbb{F}) = \mathbb{F}[x_1, \ldots, x_n]_d$
- $\partial_1, \ldots, \partial_n$ indeterminates acting on $S_{n,d}(\mathbb{F})$ as **partial derivatives**:

$$\partial_i \circ f := \frac{\partial}{\partial x_i} f, \qquad \forall\, f \in S_{n,d}(\mathbb{F})$$

The Ring of Homogeneous Differentials

- $S_{n,d}(\mathbb{F}) = \mathbb{F}[x_1, \ldots, x_n]_d$
- $\partial_1, \ldots, \partial_n$ indeterminates acting on $S_{n,d}(\mathbb{F})$ as **partial derivatives**:

$$\partial_i \circ f := \frac{\partial}{\partial x_i} f, \qquad \forall\, f \in S_{n,d}(\mathbb{F})$$

- $T_{n,d}(\mathbb{F}) = \mathbb{F}[\partial_1, \ldots, \partial_n]_d$

The Ring of Homogeneous Differentials

- $S_{n,d}(\mathbb{F}) = \mathbb{F}[x_1, \ldots, x_n]_d$
- $\partial_1, \ldots, \partial_n$ indeterminates acting on $S_{n,d}(\mathbb{F})$ as **partial derivatives**:

$$\partial_i \circ f := \frac{\partial}{\partial x_i} f, \qquad \forall\, f \in S_{n,d}(\mathbb{F})$$

- $T_{n,d}(\mathbb{F}) = \mathbb{F}[\partial_1, \ldots, \partial_n]_d$
- For each $a \leq d$ there is an $\mathbb{F}$-bilinear map

$$\begin{array}{ccc} S_{n,d}(\mathbb{F}) \times T_{n,a}(\mathbb{F}) & \longrightarrow & S_{n,d-a}(\mathbb{F}) \\ (f, D) & \longmapsto & D \circ f \end{array}$$

Catalecticant Matrices

Definition

- Let $m = \binom{n+d-2}{d-1}$,
- Let $z_1, \ldots, z_m$ be the monomial basis of $S_{n,d-1}(\mathbb{F})$ ordered lexicographically.

The **first catalecticant matrix** of $f \in S_{n,d}(\mathbb{F})$ is the matrix $C_f \in \mathbb{F}^{n \times m}$, where

$$\partial_i \circ f = \sum_{j=1}^{m} (C_f)_{i,j} z_j, \qquad \forall\, i \in [n]$$

Carlini's Result

Theorem (Carlini 2006)

Let $f \in S_{n,d}(\mathbb{F})$ and assume that $\mathbf{char}(\mathbb{F}) = 0$ or $\mathbf{char}(\mathbb{F}) > d$. Then:

(1) $\mathbf{ess}(f) = \mathrm{rk}(C_f)$

(2) $V_{\mathrm{ess}}(f) = \{D \circ f \mid D \in T_{n,d-1}(\mathbb{F})\}$

Carlini's Result

Theorem (Carlini 2006)

Let $f \in S_{n,d}(\mathbb{F})$ and assume that $\mathbf{char}(\mathbb{F}) = 0$ or $\mathbf{char}(\mathbb{F}) > d$. Then:

(1) $\mathbf{ess}(f) = \mathrm{rk}(C_f)$

(2) $V_{\mathrm{ess}}(f) = \{D \circ f \mid D \in T_{n,d-1}(\mathbb{F})\}$

The map

$$\begin{array}{ccc} (S_{n,d}(\mathbb{F}), \mathsf{d}_{\mathsf{ess}}) & \longrightarrow & (\mathbb{F}^{n \times \binom{n+d-2}{d-1}}, \mathsf{d}_{\mathsf{rk}}) \\ f & \longmapsto & C_f \end{array}$$

is an $\mathbb{F}$**-linear isometric embedding**.

Back to the Example

$$f = 3x_1^3 + 8x_1^2x_2 + 5x_1^2x_3 + 12x_1x_2^2 + 4x_1x_2x_3 + 4x_1x_3^2 + 8x_2^3 + 2x_2x_3^2 + x_3^3$$

Assume $\mathbf{char}(\mathbb{F}) \neq 2, 3$

Back to the Example

$$f = 3x_1^3 + 8x_1^2x_2 + 5x_1^2x_3 + 12x_1x_2^2 + 4x_1x_2x_3 + 4x_1x_3^2 + 8x_2^3 + 2x_2x_3^2 + x_3^3$$

Assume $\mathrm{char}(\mathbb{F}) \neq 2, 3$

$$\begin{aligned}
\partial_1 \circ f &= 9x_1^2 + 16x_1x_2 + 10x_1x_3 + 12x_2^2 + 4x_2x_3 + 4x_3^2, \\
\partial_2 \circ f &= 8x_1^2 + 24x_1x_2 + 4x_1x_3 + 24x_2^2 + 2x_3^2, \\
\partial_3 \circ f &= 5x_1^2 + 4x_1x_2 + 8x_1x_3 + 4x_2x_3 + 3x_3^2,
\end{aligned}$$

$$C_f = \begin{pmatrix} 9 & 16 & 10 & 12 & 4 & 4 \\ 8 & 24 & 4 & 24 & 0 & 2 \\ 5 & 4 & 8 & 0 & 4 & 3 \end{pmatrix}.$$

Back to the Example

$$f = 3x_1^3 + 8x_1^2x_2 + 5x_1^2x_3 + 12x_1x_2^2 + 4x_1x_2x_3 + 4x_1x_3^2 + 8x_2^3 + 2x_2x_3^2 + x_3^3$$

Assume $\mathrm{char}(\mathbb{F}) \neq 2, 3$

$$\begin{aligned}
\partial_1 \circ f &= 9x_1^2 + 16x_1x_2 + 10x_1x_3 + 12x_2^2 + 4x_2x_3 + 4x_3^2, \\
\partial_2 \circ f &= 8x_1^2 + 24x_1x_2 + 4x_1x_3 + 24x_2^2 + 2x_3^2, \\
\partial_3 \circ f &= 5x_1^2 + 4x_1x_2 + 8x_1x_3 + 4x_2x_3 + 3x_3^2,
\end{aligned}$$

$$C_f = \begin{pmatrix} 9 & 16 & 10 & 12 & 4 & 4 \\ 8 & 24 & 4 & 24 & 0 & 2 \\ 5 & 4 & 8 & 0 & 4 & 3 \end{pmatrix}.$$

By Carlini's Theorem, we get

$$\mathsf{ess}(f) = \mathsf{rk}(C_f) = 2$$

$$\begin{aligned}
V_{\mathsf{ess}}(f) &= \langle \partial_1^2 \circ f, \partial_1\partial_2 \circ f, \partial_2^2 \circ f, \partial_1\partial_3 \circ f, \partial_2\partial_3 \circ f, \partial_3^2 \circ f \rangle_{\mathbb{F}} \\
&= \langle x_1 + 2x_2, x_1 + x_3 \rangle_{\mathbb{F}}.
\end{aligned}$$

Columns Supports

- The space of essential variables represents a **natural notion of support**:

Columns Supports

- The space of essential variables represents a **natural notion of support**:
- For a matrix $A \in \mathrm{Mat}_{n\times m}(\mathbb{F})$, the **column support** $\mathrm{csupp}(A) \subseteq \mathbb{F}^n$ is defined as the $\mathbb{F}$-span of its columns.

Proposition

Let $f \in S_{n,d}(\mathbb{F})$ Then

$$V_{\mathsf{ess}}(f) = \mathrm{csupp}(C_f) \cdot (x_1, \ldots, x_n)$$

Part 2
Construction of (Nearly) Optimal Essential Rank Metric Codes

A Natural Pairing

- $S_{n,d}(\mathbb{F}) = \mathbb{F}[x_1, \ldots, x_n]_d$, $\quad T_{n,d}(\mathbb{F}) = \mathbb{F}[\partial_1, \ldots, \partial_n]_d$
- $\mathbf{char}(\mathbb{F}) > d$ or $\mathbf{char}(\mathbb{F}) = 0$.

A Natural Pairing

- $S_{n,d}(\mathbb{F}) = \mathbb{F}[x_1, \ldots, x_n]_d$, $\quad T_{n,d}(\mathbb{F}) = \mathbb{F}[\partial_1, \ldots, \partial_n]_d$
- $\mathbf{char}(\mathbb{F}) > d$ or $\mathbf{char}(\mathbb{F}) = 0$.

There is a natural pairing

$$\begin{array}{ccc} S_{n,d}(\mathbb{F}) \times T_{n,d}(\mathbb{F}) & \longrightarrow & \mathbb{F} \\ (f, D) & \longmapsto & D \circ f \end{array}$$

For $X \subseteq T_{n,d}(\mathbb{F})$, we define the **dual space** as

$$X^{\perp}. = \{f \in S_{n,d}(\mathbb{F}) : D \circ f = 0, \forall D \in X\} \subseteq S_{n,d}(\mathbb{F})$$

Degree d Symmetric Gabidulin Codes

- Assume $\mathbb{L}$ is a deg n cyclic Galois ext of $\mathbb{F}$. $(\mathbb{F} = \mathbb{F}_q, \mathbb{L} = \mathbb{F}_{q^n})$
- σ is a generator of $\mathbf{Gal}(\mathbb{L}/\mathbb{F})$. $(\sigma(\beta) = \beta^q)$

Degree d Symmetric Gabidulin Codes

- Assume $\mathbb{L}$ is a deg n cyclic Galois ext of $\mathbb{F}$. $(\mathbb{F} = \mathbb{F}_q, \mathbb{L} = \mathbb{F}_{q^n})$
- σ is a generator of $\mathbf{Gal}(\mathbb{L}/\mathbb{F})$. $(\sigma(\beta) = \beta^q)$
- Take d $\mathbb{F}$-bases of $\mathbb{L}$, $\alpha^{(1)}, \ldots, \alpha^{(d)} \in \mathbb{L}^n$.
- Call $\alpha^{(i)}(\partial) = \alpha^{(i)} \cdot (\partial_1, \ldots, \partial_n) \in T_{n,1}(\mathbb{L})$.

Degree d Symmetric Gabidulin Codes

- Assume $\mathbb{L}$ is a deg n cyclic Galois ext of $\mathbb{F}$. $(\mathbb{F} = \mathbb{F}_q,\ \mathbb{L} = \mathbb{F}_{q^n})$
- σ is a generator of $\mathrm{Gal}(\mathbb{L}/\mathbb{F})$. $(\sigma(\beta) = \beta^q)$
- Take d $\mathbb{F}$-bases of $\mathbb{L}$, $\alpha^{(1)}, \ldots, \alpha^{(d)} \in \mathbb{L}^n$.
- Call $\alpha^{(i)}(\partial) = \alpha^{(i)} \cdot (\partial_1, \ldots, \partial_n) \in T_{n,1}(\mathbb{L})$.
- Select $\rho \in \{2, \ldots, n-1\}$.

$$\mathcal{C}_\rho^{n,d} := \left\{ \alpha^{(1)}(\partial) \prod_{j=2}^{d} \sigma^{r_j}(\alpha^{(j)})(\partial) \;\middle|\; 0 \leq r_2, \ldots, r_d \leq \rho - 2 \right\}^{\perp} \cap S_{n,d}(\mathbb{F}).$$

is a **degree d symmetric Gabidulin code**

Properties of Degree d Symmetric Gabidulin Codes

Theorem

1. $\mathsf{d}_{\mathsf{ess}}(\mathcal{C}_{\rho}^{n,d}) = \rho$.
2. $\binom{n+d-1}{d} - n\binom{d+\rho-3}{d-1} \leq \dim_{\mathbb{F}}(\mathcal{C}_{\rho}^{n,d}) \leq \binom{n+d-1}{d}$.

Properties of Degree d Symmetric Gabidulin Codes

Theorem

1. $\mathsf{d}_{\mathsf{ess}}(\mathcal{C}_\rho^{n,d}) = \rho$.
2. $\binom{n+d-1}{d} - n\binom{d+\rho-3}{d-1} \leq \dim_{\mathbb{F}}(\mathcal{C}_\rho^{n,d}) \leq \binom{n+d-1}{d}$.

- When $d = 2$, $\mathcal{C}_\rho^{n,2}$ coincides with symmetric Gabidulin codes.

Properties of Degree d Symmetric Gabidulin Codes

Theorem

1. $\mathsf{d}_{\mathsf{ess}}(\mathcal{C}_\rho^{n,d}) = \rho$.
2. $\binom{n+d-1}{d} - n\binom{d+\rho-3}{d-1} \leq \dim_{\mathbb{F}}(\mathcal{C}_\rho^{n,d}) \leq \binom{n+d-1}{d}$.

- When $d = 2$, $\mathcal{C}_\rho^{n,2}$ coincides with symmetric Gabidulin codes.
- These codes are **(nearly) optimal**.
- They are a factor d far from Singleton bound for rank metric codes, **but**...

Properties of Degree d Symmetric Gabidulin Codes

Theorem

1. $\mathsf{d}_{\mathsf{ess}}(\mathcal{C}_\rho^{n,d}) = \rho$.
2. $\binom{n+d-1}{d} - n\binom{d+\rho-3}{d-1} \leq \dim_{\mathbb{F}}(\mathcal{C}_\rho^{n,d}) \leq \binom{n+d-1}{d}$.

- When $d = 2$, $\mathcal{C}_\rho^{n,2}$ coincides with symmetric Gabidulin codes.
- These codes are **(nearly) optimal**.
- They are a factor d far from Singleton bound for rank metric codes, **but**...
- ... we **conjecture** the degree d symmetry implies Singleton bound can be **improved by a factor** d (as Schmidt result for $d = 2$).

Properties of Degree d Symmetric Gabidulin Codes

Theorem

1. $\mathsf{d}_{\mathsf{ess}}(\mathcal{C}_\rho^{n,d}) = \rho$.
2. $\binom{n+d-1}{d} - n\binom{d+\rho-3}{d-1} \leq \dim_{\mathbb{F}}(\mathcal{C}_\rho^{n,d}) \leq \binom{n+d-1}{d}$.

- When $d = 2$, $\mathcal{C}_\rho^{n,2}$ coincides with symmetric Gabidulin codes.
- These codes are **(nearly) optimal**.
- They are a factor d far from Singleton bound for rank metric codes, **but**...
- ... we **conjecture** the degree d symmetry implies Singleton bound can be **improved by a factor** d (as Schmidt result for $d = 2$).
- Developed a **decoding algorithm** up to $\frac{\rho-1}{2}$ errors with cost (operations over $\mathbb{F}$)

$$\mathcal{O}(n^{d\omega}).$$

Applied Algebraic Geometry Perspectives

Several notions of ranks of homogeneous polynomials are studied in applied algebraic geometry. Among them: **strength (str)**, **slice rank (sl)**, **Waring rank (war)**, ...

- wide research in algebraic complexity theory.

Applied Algebraic Geometry Perspectives

Several notions of ranks of homogeneous polynomials are studied in applied algebraic geometry. Among them: **strength (str)**, **slice rank (sl)**, **Waring rank (war)**, ...

- wide research in algebraic complexity theory.

Proposition

$$\mathrm{str}(f) \leq \mathrm{sl}(f) \leq \mathrm{ess}(f) \leq \mathrm{war}(f).$$

- Find polynomials (one dimensional codes) with large strength is already a **difficult problem**!
- Can coding theory help with this?

The End

Thank you! Merci!

Grazie!

Definitions

Let $f \in S_{n,d}(\mathbb{F})$. The **strength** of f is the integer

$$\mathrm{str}(f) = \min\left\{ r \in \mathbb{N} \,\middle|\, f = \sum_{i=1}^{r} g_i h_i, g_i, h_i \in S_n(\mathbb{F}), \deg g_i, \deg h_i < d \right\}.$$

The **slice-rank** of f is the integer

$$\mathrm{sl}(f) = \min\left\{ r \in \mathbb{N} \,\middle|\, f = \sum_{i=1}^{r} \ell_i g_i, \ell_i \in S_{n,1}(\mathbb{F}), g_i \in S_{n,d-1}(\mathbb{F}) \right\}.$$

The **Waring rank** of f is the integer

$$\mathrm{war}(f) = \min\left\{ r \in \mathbb{N} \,\middle|\, f = \sum_{i=1}^{r} \lambda_i \ell_i^d, \lambda_i \in \mathbb{F}, \ell_i \in S_{n,1}(\mathbb{F}) \right\}.$$