Ferrers Diagram Rank-Metric Codes

Alessandro Neri

OpeRa2024 - February 14th, 2024







Contents

(Ferrers Diagram) Rank-Metric Codes

- Preliminary Definitions
- Link to Subspace Codes in Network Coding
- Ferrers Diagram Rank-Metric Codes

The Etzion-Silberstein (ES) Conjecture

- A Singleton Bound and the Conjecture
- An Illustrative Example: Triangular Diagrams

3 Recent Results on the ES Conjecture

A Modular Approach

Part 0 – Warm Up Linear Spaces of Matrices: A Few Questions

1. We want a linear space of $n \times n$ matrices over a field \mathbb{F} whose nonzero matrices are all invertible. $(n \ge 2)$

- **1.** We want a linear space of $n \times n$ matrices over a field \mathbb{F} whose nonzero matrices are all invertible. $(n \ge 2)$
- **Question 1.1**: What is the largest dimension?

- **1.** We want a linear space of $n \times n$ matrices over a field \mathbb{F} whose nonzero matrices are all invertible. $(n \ge 2)$
- **Question 1.1**: What is the largest dimension?
- Question 1.2: Can it have dimension larger than 1?

- **1.** We want a linear space of $n \times n$ matrices over a field \mathbb{F} whose nonzero matrices are all invertible. $(n \ge 2)$
- **Question 1.1**: What is the largest dimension?
- **Question 1.2**: Can it have dimension larger than 1?

2. We want a linear space of $n \times n$ upper triangular matrices over a field \mathbb{F} whose nonzero matrices are all invertible. $(n \ge 2)$

- **1.** We want a linear space of $n \times n$ matrices over a field \mathbb{F} whose nonzero matrices are all invertible. $(n \ge 2)$
- **Question 1.1**: What is the largest dimension?
- Question 1.2: Can it have dimension larger than 1?

- **2.** We want a linear space of $n \times n$ upper triangular matrices over a field \mathbb{F} whose nonzero matrices are all invertible. $(n \ge 2)$
- **Question 2.1**: What is the largest dimension?
- Question 2.2: Can it have dimension larger than 1?

- **1.** We want a linear space of $n \times n$ matrices over a field \mathbb{F} whose nonzero matrices are all invertible. $(n \ge 2)$
- Question 1.1: What is the largest dimension? ...
- Question 1.2: Can it have dimension larger than 1? ...

It depends on the field $\mathbb{F}!$

- **2.** We want a linear space of $n \times n$ upper triangular matrices over a field \mathbb{F} whose nonzero matrices are all invertible. $(n \ge 2)$
- **Question 2.1**: What is the largest dimension?
- Question 2.2: Can it have dimension larger than 1?

- **1.** We want a linear space of $n \times n$ matrices over a field \mathbb{F} whose nonzero matrices are all invertible. $(n \ge 2)$
- Question 1.1: What is the largest dimension? ...
- Question 1.2: Can it have dimension larger than 1? ...

It depends on the field $\mathbb{F}!$

- **2.** We want a linear space of $n \times n$ upper triangular matrices over a field \mathbb{F} whose nonzero matrices are all invertible. $(n \ge 2)$
- **Question 2.1**: What is the largest dimension? 1
- Question 2.2: Can it have dimension larger than 1? No



- **1.** We want a linear space of $n \times n$ matrices over a field \mathbb{F} whose nonzero matrices are all invertible. $(n \ge 2)$
- **Question 1.1**: What is the largest dimension?



- **1.** We want a linear space of $n \times n$ matrices over a field \mathbb{F} whose nonzero matrices are all invertible. $(n \ge 2)$
- Question 1.1: What is the largest dimension?

(A) If $\mathbb{F} = \mathbb{C}$ (B) If $\mathbb{F} = \mathbb{R}$ (C) If $\mathbb{F} = \mathbb{Q}$

(D) If $\mathbb{F} = \mathbb{F}_q$



- **1.** We want a linear space of $n \times n$ matrices over a field \mathbb{F} whose nonzero matrices are all invertible. $(n \ge 2)$
- **Question 1.1**: What is the largest dimension?

(A) If
$$\mathbb{F} = \mathbb{C} \longrightarrow 1$$

(B) If $\mathbb{F} = \mathbb{R}$
(C) If $\mathbb{F} = \mathbb{Q}$
(D) If $\mathbb{F} = \mathbb{F}_q$



- **1.** We want a linear space of $n \times n$ matrices over a field \mathbb{F} whose nonzero matrices are all invertible. $(n \ge 2)$
- **Question 1.1**: What is the largest dimension?

(A) If
$$\mathbb{F} = \mathbb{C} \longrightarrow 1$$

(B) If $\mathbb{F} = \mathbb{R} \longrightarrow \rho(n)$ *n*-th Radon-Hurwitz number
(C) If $\mathbb{F} = \mathbb{Q}$
(D) If $\mathbb{F} = \mathbb{F}_q$



- **1.** We want a linear space of $n \times n$ matrices over a field \mathbb{F} whose nonzero matrices are all invertible. $(n \ge 2)$
- **Question 1.1**: What is the largest dimension?

(A) If
$$\mathbb{F} = \mathbb{C} \longrightarrow 1$$

(B) If $\mathbb{F} = \mathbb{R} \longrightarrow \rho(n)$ *n*-th Radon-Hurwitz number
(C) If $\mathbb{F} = \mathbb{Q} \longrightarrow n$
(D) If $\mathbb{F} = \mathbb{F}_q$



- **1.** We want a linear space of $n \times n$ matrices over a field \mathbb{F} whose nonzero matrices are all invertible. $(n \ge 2)$
- Question 1.1: What is the largest dimension?
- (A) If $\mathbb{F} = \mathbb{C} \longrightarrow 1$ (B) If $\mathbb{F} = \mathbb{R} \longrightarrow \rho(n)$ (C) If $\mathbb{F} = \mathbb{Q} \longrightarrow n$ (D) If $\mathbb{F} = \mathbb{F}_{q} \longrightarrow n$

n-th Radon-Hurwitz number



- **1.** We want a linear space of $n \times n$ matrices over a field \mathbb{F} whose nonzero matrices are all invertible. $(n \ge 2)$
- Question 1.1: What is the largest dimension?
- (A) If $\mathbb{F} = \mathbb{C} \longrightarrow 1$ (B) If $\mathbb{F} = \mathbb{R} \longrightarrow \rho(n)$ (C) If $\mathbb{F} = \mathbb{Q} \longrightarrow n$ (D) If $\mathbb{F} = \mathbb{F}_q \longrightarrow n$

n-th Radon-Hurwitz number

1. We want a linear space of $n \times n$ matrices over a field \mathbb{F} whose nonzero matrices have rank at least r. $(n \ge r)$

- **1.** We want a linear space of $n \times n$ matrices over a field \mathbb{F} whose nonzero matrices have rank at least r. $(n \ge r)$
- Question 1.1: What is the largest dimension?

- **1.** We want a linear space of $n \times n$ matrices over a field \mathbb{F} whose nonzero matrices have rank at least r. $(n \ge r)$
- Question 1.1: What is the largest dimension?

- **1.** We want a linear space of $n \times n$ matrices over a field \mathbb{F} whose nonzero matrices have rank at least r. $(n \ge r)$
- Question 1.1: What is the largest dimension?

2. We want a linear space of $n \times n$ upper triangular matrices over a field \mathbb{F} whose nonzero matrices have rank at least r. $(n \ge r)$

- **1.** We want a linear space of $n \times n$ matrices over a field \mathbb{F} whose nonzero matrices have rank at least r. $(n \ge r)$
- Question 1.1: What is the largest dimension?

- **2.** We want a linear space of $n \times n$ upper triangular matrices over a field \mathbb{F} whose nonzero matrices have rank at least r. $(n \ge r)$
- Question 2.1: What is the largest dimension?

- **1.** We want a linear space of $n \times n$ matrices over a field \mathbb{F} whose nonzero matrices have rank at least r. $(n \ge r)$
- Question 1.1: What is the largest dimension? ...

It depends on the field $\mathbb{F}!$

- **2.** We want a linear space of $n \times n$ upper triangular matrices over a field \mathbb{F} whose nonzero matrices have rank at least r. $(n \ge r)$
- **Question 2.1**: What is the largest dimension?

- **1.** We want a linear space of $n \times n$ matrices over a field \mathbb{F} whose nonzero matrices have rank at least r. $(n \ge r)$
- Question 1.1: What is the largest dimension? ...

It depends on the field $\mathbb{F}!$

- **2.** We want a linear space of $n \times n$ upper triangular matrices over a field \mathbb{F} whose nonzero matrices have rank at least r. $(n \ge r)$
- **Question 2.1**: What is the largest dimension?

$$\frac{(n-r+1)(n-r+2)}{2}.$$

▶ (Etzion, Gorla, Ravagnani, Wachter Zeh 2016) if |F| ≥ n − 1;
 ▶ (N., Stanojkovski 2023) for every F.

Part I (Ferrers Diagram) Rank-Metric Codes

Contents

(Ferrers Diagram) Rank-Metric Codes

- Preliminary Definitions
- Link to Subspace Codes in Network Coding
- Ferrers Diagram Rank-Metric Codes

2 The Etzion-Silberstein (ES) Conjecture

- A Singleton Bound and the Conjecture
- An Illustrative Example: Triangular Diagrams

3 Recent Results on the ES Conjecture

A Modular Approach

The **rank distance** d_{rk} on $\mathbb{F}^{n \times m}$ is defined by

$$d_{\mathrm{rk}}(X, Y) := \mathrm{rk}(X - Y), \quad X, Y \in \mathbb{F}^{n \times m}.$$

The **rank distance** d_{rk} on $\mathbb{F}^{n \times m}$ is defined by (D

$$d_{\mathrm{rk}}(X, Y) := \mathrm{rk}(X - Y), \quad X, Y \in \mathbb{F}^{n \times m}$$

A $[n \times m, k, r]_{\mathbb{F}}$ rank-metric code C is a *k*-dimensional subspace of $\mathbb{F}^{n \times m}$ endowed with the rank distance. The minimum rank distance *r* is equal to the minimum rank

$$\mathbf{r} = \min\{ \mathsf{rk}(A) \mid A \in \mathcal{C} \setminus \{0\} \}.$$

The **rank distance** d_{rk} on $\mathbb{F}^{n \times m}$ is defined by (Defined by

$$d_{\mathrm{rk}}(X, Y) := \mathrm{rk}(X - Y), \quad X, Y \in \mathbb{F}^{n \times m}$$

A $[n \times m, k, r]_{\mathbb{F}}$ rank-metric code C is a *k*-dimensional subspace of $\mathbb{F}^{n \times m}$ endowed with the rank distance. The minimum rank distance *r* is equal to the minimum rank

$$\mathbf{r} = \min\{ \mathsf{rk}(A) \mid A \in \mathcal{C} \setminus \{0\} \}.$$

Singleton-like bound: $k \le \max\{n, m\}(\min\{n, m\} - r + 1).$

The **rank distance** d_{rk} on $\mathbb{F}^{n \times m}$ is defined by (Del

$$d_{\mathrm{rk}}(X, Y) := \mathrm{rk}(X - Y), \quad X, Y \in \mathbb{F}^{n \times m}$$

A $[n \times m, k, r]_{\mathbb{F}}$ rank-metric code C is a *k*-dimensional subspace of $\mathbb{F}^{n \times m}$ endowed with the rank distance. The minimum rank distance *r* is equal to the minimum rank

$$\mathbf{r} = \min\{ \mathsf{rk}(A) \mid A \in \mathcal{C} \setminus \{0\} \}.$$

Singleton-like bound: $k \le \max\{n, m\}(\min\{n, m\} - r + 1)$.

N.B. We could also consider nonlinear rank-metric codes. But not in this talk.

<u>**MRD Codes:**</u> $k = \max\{n, m\}(\min\{n, m\} - r + 1).$

<u>**MRD Codes:**</u> $k = \max\{n, m\}(\min\{n, m\} - r + 1).$

Question: How to construct MRD codes?

<u>**MRD Codes:**</u> $k = \max\{n, m\}(\min\{n, m\} - r + 1).$

Question: How to construct MRD codes?

 Constructing MRD codes with n = m for every r implies constructing MRD codes also in the rectangular case (e.g. n > m).



<u>**MRD Codes:**</u> $k = \max\{n, m\}(\min\{n, m\} - r + 1).$

Question: How to construct MRD codes?

- Constructing MRD codes with n = m for every r implies constructing MRD codes also in the rectangular case (e.g. n > m).
- Remove the last n m columns (**puncturing**) from an $[n \times n, n(n (r + (n m)) + 1), r + (n m)]_{\mathbb{F}}$ MRD code.



<u>**MRD Codes:**</u> $k = \max\{n, m\}(\min\{n, m\} - r + 1).$

Question: How to construct MRD codes?

- Constructing MRD codes with n = m for every r implies constructing MRD codes also in the rectangular case (e.g. n > m).
- Remove the last n m columns (**puncturing**) from an $[n \times n, n(n (r + (n m)) + 1), r + (n m)]_{\mathbb{F}}$ MRD code.



It is enough to do it in the square case.

Delsarte-Gabidulin Codes (I)

$$k \leq n(n-r+1).$$
Delsarte-Gabidulin Codes (I)

$$k=n(n-r+1).$$

The bound is tight over finite fields:

Preliminary Definitions

Delsarte-Gabidulin Codes (I)

$$k=n(n-r+1).$$

The bound is tight over finite fields:

•
$$\mathbb{F} = \mathbb{F}_q$$
; • $\mathbb{L} = \mathbb{F}_{q^n}$; • $\langle \sigma \rangle = \mathsf{Gal}(\mathbb{L}/\mathbb{F})$; • $\sigma(\beta) = \beta^q$

Skew-Algebra Isomorphism

$$\bigoplus_{i=0}^{n-1} \mathbb{L} \cdot \sigma^i =: \mathbb{L}[\sigma] \cong \mathsf{End}_{\mathbb{F}}(\mathbb{L}) \cong \mathbb{F}^{n \times n}$$

Preliminary Definitions

Delsarte-Gabidulin Codes (I)

$$k=n(n-r+1).$$

The bound is tight over finite fields:

•
$$\mathbb{F} = \mathbb{F}_q$$
; • $\mathbb{L} = \mathbb{F}_{q^n}$; • $\langle \sigma \rangle = \mathsf{Gal}(\mathbb{L}/\mathbb{F})$; • $\sigma(\beta) = \beta^q$

Skew-Algebra Isomorphism

$$\bigoplus_{i=0}^{n-1} \mathbb{L} \cdot \sigma^i =: \mathbb{L}[\sigma] \cong \mathsf{End}_{\mathbb{F}}(\mathbb{L}) \cong \mathbb{F}^{n \times n}$$

$$P(\sigma) = \sum_{i=0}^{n-1} a_i \sigma^i \longmapsto \left(\beta \longmapsto \sum_{i=0}^{n-1} a_i \sigma^i(\beta) \right).$$

(Artin's Theorem of independence of characters)

Alessandro Neri (UGent)

Preliminary Definitions

Delsarte-Gabidulin Codes (I)

$$k=n(n-r+1).$$

The bound is tight over finite fields:

•
$$\mathbb{F} = \mathbb{F}_q$$
; • $\mathbb{L} = \mathbb{F}_{q^n}$; • $\langle \sigma \rangle = \mathsf{Gal}(\mathbb{L}/\mathbb{F})$; • $\sigma(\beta) = \beta^q$

Skew-Algebra Isomorphism

$$\bigoplus_{i=0}^{n-1} \mathbb{L} \cdot \mathbf{x}^{q^i} =: \mathcal{L}_{n,q}[\mathbf{x}] \cong \mathsf{End}_{\mathbb{F}}(\mathbb{L}) \cong \mathbb{F}^{n \times n}$$

$$P(\mathbf{x}) = \sum_{i=0}^{n-1} a_i \mathbf{x}^{q^i} \longmapsto \left(\beta \longmapsto \sum_{i=0}^{n-1} a_i \beta^{q^i} \right)$$

(Artin's Theorem of independence of characters) (Linearized Polynomials)

.

Delsarte-Gabidulin Codes (II)

Nullity-Degree Bound

If $P(\sigma) \in \mathbb{L}[\sigma]$ is nonzero, then

 $\dim_{\mathbb{F}}(\ker(P)) \leq \deg_{\sigma}(P).$

(Artin's Theorem of independence of characters)

Delsarte-Gabidulin Codes (II)

Nullity-Degree Bound

If $P(\sigma) \in \mathbb{L}[\sigma]$ is nonzero, then

 $\operatorname{rk}(P) \geq n - \operatorname{deg}_{\sigma}(P).$

(Artin's Theorem of independence of characters)

Delsarte-Gabidulin Codes (II)

Nullity-Degree Bound

If $P(\sigma) \in \mathbb{L}[\sigma]$ is nonzero, then

 $\mathsf{rk}(P) \ge n - \mathsf{deg}_{\sigma}(P).$

(Artin's Theorem of independence of characters)

Delsarte-Gabidulin construction: (Delsarte, 1978 - Gabidulin, 1985 - ...)

$$\mathbb{L}[\sigma]_{n-r} := \bigoplus_{i=0}^{n-r} \mathbb{L} \cdot \sigma^i$$

is (isomorphic to) an $[n \times n, n(n - r + 1), r]_{\mathbb{F}}$ code.

Communication Through a Network

Question: Why do we care about rank-metric codes?

Communication Through a Network

Question: Why do we care about rank-metric codes?



Routing vs. Network Coding

Routing:

- Nodes can only forward packets
- If two packets are received, one has to be discarded



Routing vs. Network Coding

Routing:

- Nodes can only forward packets
- If two packets are received, one has to be discarded



Network coding:

- Nodes can forward linear combinations
- ⇒ higher throughput achievable!



Example



Example



Receiver R_1 and Receiver R_2 get, respectively, the following packets:

$$\begin{array}{c} a \\ a + b \\ b + c \end{array} \right) = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix}, \qquad \begin{pmatrix} a + b \\ b + c \\ c \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix}.$$

Example



Receiver R_1 and Receiver R_2 get, respectively, the following packets:

$$\begin{pmatrix} a \\ a+b \\ b+c \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix}, \qquad \begin{pmatrix} a+b \\ b+c \\ c \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ b \\ c \end{pmatrix}.$$

N.B. What is sent and what is received have the same 3-dim'l rowspace

Example: An Error Occurs



Thus, Receiver R_1 and Receiver R_2 actually get, respectively:

$$\begin{array}{c} a \\ a + x \\ \times + c \end{array} \right) = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} a \\ x \\ c \\ c \end{array} \right), \qquad \begin{pmatrix} a + x \\ x + c \\ c \\ c \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ x \\ c \\ c \end{pmatrix}$$

Example: An Error Occurs



Thus, Receiver R_1 and Receiver R_2 actually get, respectively:

$$\begin{pmatrix} a \\ a+x \\ x+c \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \begin{pmatrix} a \\ x \\ c \end{pmatrix}, \qquad \begin{pmatrix} a+x \\ x+c \\ c \end{pmatrix} = \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} a \\ x \\ c \end{pmatrix}$$

N.B. The two rowspaces still share a 2-dim'l subspace.

(Koetter, Kschischang, 2008)

A (constant dimension) subspace code is a subset of the Grassmannian $\mathcal{G}_{\mathbb{F}}(n, n+m)$ endowed with the

Injection Distance: $d_{I}(\mathcal{U}, \mathcal{V}) := n - \dim_{\mathbb{F}}(\mathcal{U} \cap \mathcal{V})$

(Koetter, Kschischang, 2008)

A (constant dimension) subspace code is a subset of the Grassmannian $\mathcal{G}_{\mathbb{F}}(n, n+m)$ endowed with the

Injection Distance: $d_{I}(\mathcal{U}, \mathcal{V}) := n - \dim_{\mathbb{F}}(\mathcal{U} \cap \mathcal{V})$

Isometric embedding:

(Silva, Koetter, Kschischang, 2008)

$$\begin{array}{ccc} (\mathbb{F}^{n \times m}, \mathsf{d}_{\mathsf{rk}}) & \longleftrightarrow & (\mathcal{G}_{\mathbb{F}}(n, n+m), \mathsf{d}_{\mathsf{I}}) \\ A & \longmapsto & \operatorname{rowsp}(\operatorname{Id}_n | A) \end{array}$$

(Koetter, Kschischang, 2008)

A (constant dimension) subspace code is a subset of the Grassmannian $\mathcal{G}_{\mathbb{F}}(n, n+m)$ endowed with the

Injection Distance: $d_{I}(\mathcal{U}, \mathcal{V}) := n - \dim_{\mathbb{F}}(\mathcal{U} \cap \mathcal{V})$

Isometric embedding:

(Silva, Koetter, Kschischang, 2008)

$$\begin{array}{ccc} (\mathbb{F}^{n \times m}, \mathsf{d}_{\mathsf{rk}}) & \hookrightarrow & (\mathcal{G}_{\mathbb{F}}(n, n+m), \mathsf{d}_{\mathsf{I}}) \\ A & \longmapsto & \operatorname{rowsp}(\operatorname{Id}_{n} | A) \end{array}$$

 $d_{I}(rowsp(Id_{n} | A), rowsp(Id_{n} | B)) = d_{rk}(A, B) = rk(A - B)$

(Koetter, Kschischang, 2008)

A (constant dimension) subspace code is a subset of the Grassmannian $\mathcal{G}_{\mathbb{F}}(n, n+m)$ endowed with the

Injection Distance: $d_{I}(\mathcal{U}, \mathcal{V}) := n - \dim_{\mathbb{F}}(\mathcal{U} \cap \mathcal{V})$

Isometric embedding:

(Silva, Koetter, Kschischang, 2008)

$$\begin{array}{ccc} (\mathbb{F}^{n \times m}, \mathsf{d}_{\mathsf{rk}}) & \hookrightarrow & (\mathcal{G}_{\mathbb{F}}(n, n+m), \mathsf{d}_{\mathsf{I}}) \\ A & \longmapsto & \operatorname{rowsp}(\operatorname{Id}_n | A) \end{array}$$

 $d_{I}(rowsp(Id_{n} | A), rowsp(Id_{n} | B)) = d_{rk}(A, B) = rk(A - B)$

Natural notion of F-linearity

Cell Decomposition of the Grassmannian

The above embedding can be generalized.

• Every $\mathcal{U} \in \mathcal{G}_{\mathbb{F}}(n, n + m)$ has a unique Reduced Row Echelon Form. This gives a set of pivot positions.

Cell Decomposition of the Grassmannian

The above embedding can be generalized.

- Every U ∈ G_F(n, n + m) has a unique Reduced Row Echelon Form. This gives a set of pivot positions.
- The space G_𝔅(n, n + m) can be partitioned into (^{n+m}_n) Schubert cells according to the n pivot positions of the subspaces.

Cell Decomposition of the Grassmannian

The above embedding can be generalized.

- Every U ∈ G_F(n, n + m) has a unique Reduced Row Echelon Form. This gives a set of pivot positions.
- The space G_𝔅(n, n + m) can be partitioned into (^{n+m}_n) Schubert cells according to the n pivot positions of the subspaces.
- To each set of *n* pivot positions, we can associate a **Ferrers** diagram¹, and a **Ferrers** diagram matrix space¹!

¹yet to be defined

$$n = m = 5;$$
 pivots $P = \{2, 5, 6, 7, 9\}$

$$n = m = 5;$$
 pivots $P = \{2, 5, 6, 7, 9\}$

$$\mathcal{G}_{\mathbb{F}}^{P}(5,10) = \left\{ rs \begin{pmatrix} 0 & 1 & a_{1,2} & a_{1,3} & 0 & 0 & 0 & a_{1,4} & 0 & a_{1,5} \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & a_{2,4} & 0 & a_{2,5} \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & a_{3,4} & 0 & a_{3,5} \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & a_{4,4} & 0 & a_{4,5} \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & a_{5,5} \end{pmatrix} : a_{i,j} \in \mathbb{F} \right\}$$

n = m = 5; pivots $P = \{2, 5, 6, 7, 9\}$

n = m = 5; pivots $P = \{2, 5, 6, 7, 9\}$

$$\mathcal{G}_{\mathbb{F}}^{P}(5,10) = \left\{ rs \begin{pmatrix} 0 & 1 & \bullet & \bullet & 0 & 0 & \bullet & 0 & \bullet \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & \bullet & 0 & \bullet \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & \bullet & 0 & \bullet \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & \bullet & 0 & \bullet \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \bullet & \end{pmatrix} \right\}$$



n = m = 5; pivots $P = \{2, 5, 6, 7, 9\}$

$$\mathcal{G}_{\mathbb{F}}^{P}(5,10) = \left\{ rs \begin{pmatrix} 0 & 1 & \bullet & 0 & 0 & 0 & \bullet & 0 & \bullet \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & \bullet & 0 & \bullet \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & \bullet & 0 & \bullet \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & \bullet & 0 & \bullet \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \bullet \end{pmatrix} \right\}$$



Isometry (Etzion, Silberstein 2009)

$$(\mathcal{G}_{\mathbb{F}}^{P}(n,2n),d_{I})\cong (\mathbb{F}^{\mathcal{D}_{P}},d_{rk})$$

n = m = 5; pivots $P = \{2, 5, 6, 7, 9\}$

$$\mathcal{G}_{\mathbb{F}}^{P}(5,10) = \left\{ rs \begin{pmatrix} 0 & 1 & \bullet & 0 & 0 & 0 & \bullet & 0 & \bullet \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & \bullet & 0 & \bullet \\ 0 & 0 & 0 & 0 & 0 & 1 & 0 & \bullet & 0 & \bullet \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & \bullet & 0 & \bullet \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & \bullet \end{pmatrix} \right\}$$



Isometry (Etzion, Silberstein 2009)

 $(\mathcal{G}_{\mathbb{F}}^{\mathcal{P}}(n,2n),d_{\mathrm{I}})\cong (\mathbb{F}^{\mathcal{D}_{\mathcal{P}}},d_{\mathrm{rk}})$

- Natural notion of \mathbb{F} -linearity
- Multilevel construction for subspace codes (Etzion, Silberstein 2009)

- $\mathcal{D} \neq \emptyset$;
- If $(i, j) \in \mathcal{D}$, then $(i, j') \in \mathcal{D}$ for every $j' \in \{j, \ldots, n\}$;
- If $(i, j) \in \mathcal{D}$, then $(i', j) \in \mathcal{D}$ for every $i' \in \{1, \ldots, i\}$.

•
$$\mathcal{D} \neq \emptyset$$
;

- If $(i, j) \in \mathcal{D}$, then $(i, j') \in \mathcal{D}$ for every $j' \in \{j, \ldots, n\}$;
- If $(i, j) \in \mathcal{D}$, then $(i', j) \in \mathcal{D}$ for every $i' \in \{1, \ldots, i\}$.



•
$$\mathcal{D} \neq \emptyset$$
;

- If $(i, j) \in \mathcal{D}$, then $(i, j') \in \mathcal{D}$ for every $j' \in \{j, \ldots, n\}$;
- If $(i, j) \in \mathcal{D}$, then $(i', j) \in \mathcal{D}$ for every $i' \in \{1, \ldots, i\}$.



•
$$\mathcal{D} \neq \emptyset$$
;

- If $(i, j) \in \mathcal{D}$, then $(i, j') \in \mathcal{D}$ for every $j' \in \{j, \ldots, n\}$;
- If $(i, j) \in \mathcal{D}$, then $(i', j) \in \mathcal{D}$ for every $i' \in \{1, \ldots, i\}$.



•
$$\mathcal{D} \neq \emptyset$$
;

- If $(i, j) \in \mathcal{D}$, then $(i, j') \in \mathcal{D}$ for every $j' \in \{j, \ldots, n\}$;
- If $(i, j) \in \mathcal{D}$, then $(i', j) \in \mathcal{D}$ for every $i' \in \{1, \ldots, i\}$.



•
$$\mathcal{D} \neq \emptyset$$
;

- If $(i, j) \in \mathcal{D}$, then $(i, j') \in \mathcal{D}$ for every $j' \in \{j, \ldots, n\}$;
- If $(i, j) \in \mathcal{D}$, then $(i', j) \in \mathcal{D}$ for every $i' \in \{1, \ldots, i\}$.



•
$$\mathcal{D} \neq \emptyset$$
;

- If $(i, j) \in \mathcal{D}$, then $(i, j') \in \mathcal{D}$ for every $j' \in \{j, \ldots, n\}$;
- If $(i, j) \in \mathcal{D}$, then $(i', j) \in \mathcal{D}$ for every $i' \in \{1, \ldots, i\}$.


Ferrers Diagrams

A **Ferrers diagram** \mathcal{D} of order *n* is a subset of $[n]^2$ s.t.:

•
$$\mathcal{D} \neq \emptyset$$
;

- If $(i, j) \in \mathcal{D}$, then $(i, j') \in \mathcal{D}$ for every $j' \in \{j, \ldots, n\}$;
- If $(i, j) \in \mathcal{D}$, then $(i', j) \in \mathcal{D}$ for every $i' \in \{1, \ldots, i\}$.



Subset of
$$[n]^2$$
 Graphical Repr.
 $\mathcal{D} = \{(1, 2), (1, 3), (1, 4), (1, 5), (2, 4), (2, 5), (3, 4), (3, 5), (4, 4), (4, 5), (5, 5)\}$













Ferrers Diagram Matrix Spaces

- (Finite) field \mathbb{F} .
- Ferrers diagram \mathcal{D} of order n.

Ferrers Diagram Matrix Spaces

- (Finite) field \mathbb{F} .
- Ferrers diagram \mathcal{D} of order n.

$$\mathbb{F}^{\mathcal{D}} := \{ A \in \mathbb{F}^{n \times n} : a_{ij} = 0 \ \forall (i, j) \notin \mathcal{D} \}.$$

Ferrers Diagram Matrix Spaces

- (Finite) field \mathbb{F} .
- Ferrers diagram \mathcal{D} of order n.

$$\mathbb{F}^{\mathcal{D}} := \{ A \in \mathbb{F}^{n \times n} : a_{ij} = 0 \ \forall (i, j) \notin \mathcal{D} \}.$$



The rank distance d_{rk} on $\mathbb{F}^{n \times n}$ is defined by

$$d_{\mathrm{rk}}(X, Y) := \mathrm{rk}(X - Y), \quad X, Y \in \mathbb{F}^{n \times n}$$

The rank distance d_{rk} on $\mathbb{F}^{\mathcal{D}}$ is defined by

$$\mathrm{d}_{\mathrm{rk}}(X,Y) := \mathrm{rk}(X-Y), \quad X, Y \in \mathbb{F}^{\mathcal{D}}.$$

The rank distance d_{rk} on $\mathbb{F}^{\mathcal{D}}$ is defined by

$$d_{\mathrm{rk}}(X, Y) := \mathrm{rk}(X - Y), \quad X, Y \in \mathbb{F}^{\mathcal{D}}.$$

A $[\mathcal{D}, k, r]_{\mathbb{F}}$ Ferrers diagram rank-metric code \mathcal{C} is a *k*-dimensional subspace of $\mathbb{F}^{\mathcal{D}}$ endowed with the rank distance. The **minimum rank** distance *r* is equal to the **minimum rank**

 $\mathbf{r} = \min\{ \mathsf{rk}(A) \mid A \in \mathcal{C} \setminus \{0\} \}.$

The rank distance d_{rk} on $\mathbb{F}^{\mathcal{D}}$ is defined by

$$d_{\mathrm{rk}}(X, Y) := \mathrm{rk}(X - Y), \quad X, Y \in \mathbb{F}^{\mathcal{D}}.$$

A $[\mathcal{D}, k, r]_{\mathbb{F}}$ Ferrers diagram rank-metric code \mathcal{C} is a *k*-dimensional subspace of $\mathbb{F}^{\mathcal{D}}$ endowed with the rank distance. The **minimum rank** distance *r* is equal to the **minimum rank**

 $\mathbf{r} = \min\{\mathsf{rk}(A) \mid A \in \mathcal{C} \setminus \{0\}\}.$

N.B. We could also consider nonlinear Ferrers diagram rank-metric codes. But not in this talk.

Part II The Etzion-Silberstein Conjecture

Contents

(Ferrers Diagram) Rank-Metric Codes

- Preliminary Definitions
- Link to Subspace Codes in Network Coding
- Ferrers Diagram Rank-Metric Codes

The Etzion-Silberstein (ES) Conjecture

- A Singleton Bound and the Conjecture
- An Illustrative Example: Triangular Diagrams

3 Recent Results on the ES Conjecture

A Modular Approach

Question: Let $\mathcal{D} = (c_1, \ldots, c_n)$ be a Ferrers diagram, $2 \le r \le n$. Find

 $\kappa_{\mathbb{F}}(\mathcal{D}, r) = \max\{k \in \mathbb{N} : \exists \text{ an } [\mathcal{D}, k, r]_{\mathbb{F}} \text{ code } \}.$

Question: Let $\mathcal{D} = (c_1, \ldots, c_n)$ be a Ferrers diagram, $2 \le r \le n$. Find

 $\kappa_{\mathbb{F}}(\mathcal{D}, r) = \max\{k \in \mathbb{N} : \exists an [\mathcal{D}, k, r]_{\mathbb{F}} \text{ code } \}.$

Singleton-like Bound (Etzion, Silberstein, 2009)

$$\kappa_{\mathbb{F}}(\mathcal{D}, r) \leq \nu_{\min}(\mathcal{D}, r) := \min_{0 \leq j < r} \nu_j(\mathcal{D}, r)$$

Question: Let $\mathcal{D} = (c_1, \ldots, c_n)$ be a Ferrers diagram, $2 \le r \le n$. Find

 $\kappa_{\mathbb{F}}(\mathcal{D}, r) = \max\{k \in \mathbb{N} : \exists an [\mathcal{D}, k, r]_{\mathbb{F}} \text{ code } \}.$

Singleton-like Bound (Etzion, Silberstein, 2009)

$$\begin{aligned} \kappa_{\mathbb{F}}(\mathcal{D},r) &\leq \nu_{\min}(\mathcal{D},r) := \min_{0 \leq j < r} \nu_j(\mathcal{D},r) \\ &= \min_{0 \leq j < r} \Big\{ \sum_{i=1}^{n-j} \max\{0, c_i - r + 1 + j\} \end{aligned}$$

Question: Let $\mathcal{D} = (c_1, \ldots, c_n)$ be a Ferrers diagram, $2 \le r \le n$. Find

 $\kappa_{\mathbb{F}}(\mathcal{D}, r) = \max\{k \in \mathbb{N} : \exists an [\mathcal{D}, k, r]_{\mathbb{F}} \text{ code } \}.$

Singleton-like Bound (Etzion, Silberstein, 2009)

$$\kappa_{\mathbb{F}}(\mathcal{D}, r) \leq \nu_{\min}(\mathcal{D}, r) := \min_{0 \leq j < r} \nu_j(\mathcal{D}, r)$$
$$= \min_{0 \leq j < r} |\mathcal{D}| - |(\{ \text{ dots in first } r - j - 1 \text{ rows}\} \cup \{ \text{ dots in last } j \text{ col's}\})|$$

Question: Let $\mathcal{D} = (c_1, \ldots, c_n)$ be a Ferrers diagram, $2 \le r \le n$. Find

$$\kappa_{\mathbb{F}}(\mathcal{D}, r) = \max\{k \in \mathbb{N} : \exists \text{ an } [\mathcal{D}, k, r]_{\mathbb{F}} \text{ code } \}.$$

Singleton-like Bound (Etzion, Silberstein, 2009)

$$\kappa_{\mathbb{F}}(\mathcal{D}, r) \leq \nu_{\min}(\mathcal{D}, r) := \min_{0 \leq i < r} \nu_j(\mathcal{D}, r)$$

 $= \min_{0 \le j < r} |\mathcal{D}| - |(\{ \text{ dots in first } r - j - 1 \text{ rows}\} \cup \{ \text{ dots in last } j \text{ col's}\})|$



Question: Let $\mathcal{D} = (c_1, \ldots, c_n)$ be a Ferrers diagram, $2 \le r \le n$. Find

$$\kappa_{\mathbb{F}}(\mathcal{D}, r) = \max\{k \in \mathbb{N} : \exists an [\mathcal{D}, k, r]_{\mathbb{F}} \text{ code } \}.$$

Singleton-like Bound (Etzion, Silberstein, 2009)

$$\kappa_{\mathbb{F}}(\mathcal{D}, r) \leq \nu_{\min}(\mathcal{D}, r) := \min_{0 \leq i \leq r} \nu_j(\mathcal{D}, r)$$

 $= \min_{0 \le j < r} |\mathcal{D}| - |(\{ \text{ dots in first } r - j - 1 \text{ rows}\} \cup \{ \text{ dots in last } j \text{ col's}\})|$

= 5

Example:
$$r = 3$$
 $\nu_0(\mathcal{D}, 3)$

Question: Let $\mathcal{D} = (c_1, \ldots, c_n)$ be a Ferrers diagram, $2 \le r \le n$. Find

$$\kappa_{\mathbb{F}}(\mathcal{D}, r) = \max\{k \in \mathbb{N} : \exists an [\mathcal{D}, k, r]_{\mathbb{F}} \text{ code } \}.$$

Singleton-like Bound (Etzion, Silberstein, 2009)

$$\kappa_{\mathbb{F}}(\mathcal{D}, r) \leq \nu_{\min}(\mathcal{D}, r) := \min_{0 \leq i \leq r} \nu_j(\mathcal{D}, r)$$

 $= \min_{0 \le j < r} |\mathcal{D}| - |(\{ \text{ dots in first } r - j - 1 \text{ rows}\} \cup \{ \text{ dots in last } j \text{ col's}\})|$

Example:

$$r = 3$$
 $r = 3$
 $\nu_0(\mathcal{D}, 3) = 5$
 $\nu_1(\mathcal{D}, 3) = 3$

Question: Let $\mathcal{D} = (c_1, \ldots, c_n)$ be a Ferrers diagram, $2 \le r \le n$. Find

$$\kappa_{\mathbb{F}}(\mathcal{D}, r) = \max\{k \in \mathbb{N} : \exists an [\mathcal{D}, k, r]_{\mathbb{F}} \text{ code } \}.$$

Singleton-like Bound (Etzion, Silberstein, 2009)

$$\kappa_{\mathbb{F}}(\mathcal{D}, r) \leq \nu_{\min}(\mathcal{D}, r) := \min_{0 \leq i \leq r} \nu_j(\mathcal{D}, r)$$

 $= \min_{0 \le j < r} |\mathcal{D}| - |(\{ \text{ dots in first } r - j - 1 \text{ rows}\} \cup \{ \text{ dots in last } j \text{ col's}\})|$

Example:

r = 3

$$\nu_0(D, 3) = 5$$

 $\nu_1(D, 3) = 3$
 $\nu_2(D, 3) = 2$

Alessandro Neri (UGent)

Question: Let $\mathcal{D} = (c_1, \ldots, c_n)$ be a Ferrers diagram, $2 \le r \le n$. Find

$$\kappa_{\mathbb{F}}(\mathcal{D}, r) = \max\{k \in \mathbb{N} : \exists \text{ an } [\mathcal{D}, k, r]_{\mathbb{F}} \text{ code } \}.$$

Singleton-like Bound (Etzion, Silberstein, 2009)

$$\kappa_{\mathbb{F}}(\mathcal{D}, r) \leq \nu_{\min}(\mathcal{D}, r) := \min_{0 \leq i < r} \nu_j(\mathcal{D}, r)$$

 $= \min_{0 \le j < r} |\mathcal{D}| - |(\{ \text{ dots in first } r - j - 1 \text{ rows}\} \cup \{ \text{ dots in last } j \text{ col's}\})|$



 $\nu_{\min}(\mathcal{D}, r) = 2$

Etzion–Silberstein Conjecture

Etzion–Silberstein Conjecture (2009): For every finite field \mathbb{F} the Singleton-like bound is tight:

 $\kappa_{\mathbb{F}}(\mathcal{D}, r) = \nu_{\min}(\mathcal{D}, r)$

Etzion–Silberstein Conjecture

Etzion–Silberstein Conjecture (2009): For every **finite field** \mathbb{F} the Singleton-like bound is tight:

$$\kappa_{\mathbb{F}}(\mathcal{D}, r) = \nu_{\min}(\mathcal{D}, r)$$

Two constructive proofs for some special cases

- Subcodes of MRD codes: (Etzion, Silberstein, 2009) (Etzion, Gorla, Ravagnani, Wachter-Zeh, 2016) (Gorla, Ravagnani, 2017) (Antrobus, Gluesing-Luerssen, 2019) (Liu, Chang, Feng, 2019)
- (2) **MDS-constructible Ferrers diagrams** (for fields large enough): (Etzion, Gorla, Ravagnani, Wachter-Zeh, 2016)

Two Special Cases

Two Special Cases

(1) Full size diagrams: $\mathcal{D} = (n, n, \dots, n) = [n]^2$



Two Special Cases

(1) Full size diagrams: $\mathcal{D} = (n, n, \dots, n) = [n]^2$



(2) Triangular diagrams: $\mathcal{D} = (1, 2, \dots, n) = \{(i, j) \in [n]^2 : i \leq j\} = \mathcal{T}_n$

$$\mathcal{D} = (1, 2, \dots, n) = \{(i, j) \in [n]^2 : i \leq j\} = \mathcal{T}_n.$$

Upper-triangular **rank-metric codes.**

$$\nu_{\min}(\mathcal{T}_n, r) = \frac{(n-r+1)(n-r+2)}{2}$$



$$\mathcal{D} = (1, 2, \dots, n) = \{(i, j) \in [n]^2 : i \leq j\} = \mathcal{T}_n.$$

Upper-triangular **rank-metric codes.**

$$\nu_{\min}(\mathcal{T}_n,r)=\frac{(n-r+1)(n-r+2)}{2}.$$



(1) r = n: Easy.

(2)
$$r = 2$$
: Sum on each diagonal is 0.

(3) r = n - 1: Settled in (Antrobus–Gluesing Luerssen 2019).

$$\mathcal{D} = (1, 2, \dots, n) = \{(i, j) \in [n]^2 : i \leq j\} = \mathcal{T}_n.$$

Upper-triangular **rank-metric codes.**

$$u_{\min}(\mathcal{T}_n, r) = \frac{(n-r+1)(n-r+2)}{2}.$$



(1) r = n: Easy.

(2) r = 2: Sum on each diagonal is 0.

(3) r = n - 1: Settled in (Antrobus–Gluesing Luerssen 2019).

(4) For every other *r* assuming $|\mathbb{F}| \ge n - 1$.

$$\mathcal{D} = (1, 2, \dots, n) = \{(i, j) \in [n]^2 : i \leq j\} = \mathcal{T}_n.$$

Upper-triangular **rank-metric codes.**

$$\nu_{\min}(\mathcal{T}_n,r)=\frac{(n-r+1)(n-r+2)}{2}.$$



(1) r = n: Easy.

(2) r = 2: Sum on each diagonal is 0.

(3) r = n - 1: Settled in (Antrobus–Gluesing Luerssen 2019).

(4) For every other *r* assuming $|\mathbb{F}| \ge n - 1$.

How? Put $[n+1-i, n-r-i+2, r]_{\mathbb{F}}$ MDS codes on the diagonals

$$\Delta_i^n := \{ (j, j+i-1) : j \in [n+1-i] \}$$

for $i \in [n - r + 1]$.

Alessandro Neri (UGent)

(MDS-Constructible)

$$\mathcal{D} = (1, 2, \dots, n) = \{(i, j) \in [n]^2 : i \leq j\} = \mathcal{T}_n.$$

Upper-triangular **rank-metric codes.**

$$\nu_{\min}(\mathcal{T}_n,r)=\frac{(n-r+1)(n-r+2)}{2}.$$

(1) r = n: Easy.

(2) r = 2: Sum on each diagonal is 0.

(3) r = n - 1: Settled in (Antrobus–Gluesing Luerssen 2019).

(4) For every other *r* assuming $|\mathbb{F}| \ge n-1$.

How? Put $[n+1-i, n-r-i+2, r]_{\mathbb{F}}$ **MDS codes on the diagonals**

$$\Delta_i^n := \{ (j, j+i-1) : j \in [n+1-i] \}$$

for $i \in [n - r + 1]$.

Alessandro Neri (UGent)

27 / 34
A Special Case: Upper Triangular Matrices

$$\mathcal{D} = (1, 2, \dots, n) = \{(i, j) \in [n]^2 : i \leq j\} = \mathcal{T}_n.$$

Upper-triangular **rank-metric codes.**

$$\nu_{\min}(\mathcal{T}_n,r)=\frac{(n-r+1)(n-r+2)}{2}.$$



(1) r = n: Easy.

(2) r = 2: Sum on each diagonal is 0.

(3) r = n - 1: Settled in (Antrobus–Gluesing Luerssen 2019).

(4) For every other *r* assuming $|\mathbb{F}| \ge n - 1$.

How? Put $[n+1-i, n-r-i+2, r]_{\mathbb{F}}$ MDS codes on the diagonals

$$\Delta_i^n := \{ (j, j+i-1) : j \in [n+1-i] \}$$

for $i \in [n - r + 1]$.

Alessandro Neri (UGent)

(MDS-Constructible)

A Special Case: Upper Triangular Matrices

 $\mathcal{D} = (1, 2, \dots, n) = \{(i, j) \in [n]^2 : i \leq j\} = \mathcal{T}_n.$ Upper-triangular **rank-metric codes.**

$$\nu_{\min}(\mathcal{T}_n, r) = \frac{(n-r+1)(n-r+2)}{2}$$



(1) r = n: Easy.

(2)
$$r = 2$$
: Sum on each diagonal is 0.

(3) r = n - 1: Settled in (Antrobus–Gluesing Luerssen 2019).

(4) For every other *r* assuming $|\mathbb{F}| \ge n - 1$.

How? Put $[n+1-i, n-r-i+2, r]_{\mathbb{F}}$ MDS codes on the diagonals

$$\Delta_i^n := \{ (j, j+i-1) : j \in [n+1-i] \}$$

for $i \in [n - r + 1]$.

Alessandro Neri (UGent)

(MDS-Constructible)

Let \mathcal{D} be a Ferrers diagram of order n, and let $r \in \{2, \ldots, n\}$.

Formal Definition: The pair (\mathcal{D}, r) is **MDS-constructible** if

$$\nu_{\min}(\mathcal{D}, r) = \sum_{i=1}^{n} \max\{0, |\mathcal{D} \cap \Delta_i^n| - r + 1\} =: \nu_{\mathrm{MDS}}(\mathcal{D}, r).$$

Let \mathcal{D} be a Ferrers diagram of order n, and let $r \in \{2, \ldots, n\}$.

Formal Definition: The pair (\mathcal{D}, r) is **MDS-constructible** if

$$\nu_{\min}(\mathcal{D}, r) = \sum_{i=1}^{n} \max\{0, |\mathcal{D} \cap \Delta_i^n| - r + 1\} =: \nu_{\mathrm{MDS}}(\mathcal{D}, r).$$

Intuitive Definition: The pair (\mathcal{D}, r) is **MDS-constructible** if you can construct $[\mathcal{D}, \nu_{\min}(\mathcal{D}, r), r]_{\mathbb{F}}$ code using MDS codes of minimum Hamming weight r on the diagonals.

Let \mathcal{D} be a Ferrers diagram of order n, and let $r \in \{2, \ldots, n\}$.

Formal Definition: The pair (\mathcal{D}, r) is **MDS-constructible** if

$$\nu_{\min}(\mathcal{D}, r) = \sum_{i=1}^{n} \max\{0, |\mathcal{D} \cap \Delta_i^n| - r + 1\} =: \nu_{\mathrm{MDS}}(\mathcal{D}, r).$$

Intuitive Definition: The pair (\mathcal{D}, r) is **MDS-constructible** if you can construct $[\mathcal{D}, \nu_{\min}(\mathcal{D}, r), r]_{\mathbb{F}}$ code using MDS codes of minimum Hamming weight r on the diagonals.



Let \mathcal{D} be a Ferrers diagram of order n, and let $r \in \{2, \ldots, n\}$.

Formal Definition: The pair (\mathcal{D}, r) is **MDS-constructible** if

$$\nu_{\min}(\mathcal{D}, r) = \sum_{i=1}^{n} \max\{0, |\mathcal{D} \cap \Delta_i^n| - r + 1\} =: \nu_{\mathrm{MDS}}(\mathcal{D}, r).$$

Intuitive Definition: The pair (\mathcal{D}, r) is **MDS-constructible** if you can construct $[\mathcal{D}, \nu_{\min}(\mathcal{D}, r), r]_{\mathbb{F}}$ code using MDS codes of minimum Hamming weight r on the diagonals.

$$\nu_{\min}(\mathcal{D}, 3) = \min\{5, 4, 3\} = 3$$

$$\nu_{\text{MDS}}(\mathcal{D}, 3) = 0 + 2 + 1 + 0 + 0 = 3$$

Alessandro Neri (UGent)

Theorem (Etzion, Gorla, Ravagnani, Wachter-Zeh 2016)

If (\mathcal{D}, r) is MDS-constructible and $|\mathbb{F}| \geq \max_i |\mathcal{D} \cap \Delta_i^n| - 1$, then

Theorem (Etzion, Gorla, Ravagnani, Wachter-Zeh 2016)

If (\mathcal{D}, r) is MDS-constructible and $|\mathbb{F}| \geq \max_i |\mathcal{D} \cap \Delta_i^n| - 1$, then

Theorem (Etzion, Gorla, Ravagnani, Wachter-Zeh 2016)

If (\mathcal{D}, r) is MDS-constructible and $|\mathbb{F}| \geq \max_i |\mathcal{D} \cap \Delta_i^n| - 1$, then



Theorem (Etzion, Gorla, Ravagnani, Wachter-Zeh 2016)

If (\mathcal{D}, r) is MDS-constructible and $|\mathbb{F}| \geq \max_i |\mathcal{D} \cap \Delta_i^n| - 1$, then



Theorem (Etzion, Gorla, Ravagnani, Wachter-Zeh 2016)

If (\mathcal{D}, r) is MDS-constructible and $|\mathbb{F}| \geq \max_i |\mathcal{D} \cap \Delta_i^n| - 1$, then



Theorem (Etzion, Gorla, Ravagnani, Wachter-Zeh 2016)

If (\mathcal{D}, r) is MDS-constructible and $|\mathbb{F}| \geq \max_i |\mathcal{D} \cap \Delta_i^n| - 1$, then



Part III Recent Results on the ES Conjecture

Joint work with Mima Stanojkovski

Check out our preprint!

A. Neri. M. Stanojkovski. "A proof of the Etzion-Silberstein conjecture for monotone and MDS-constructible Ferrers diagrams", arXiv:2306.16407, 2023.



Contents

(Ferrers Diagram) Rank-Metric Codes

- Preliminary Definitions
- Link to Subspace Codes in Network Coding
- Ferrers Diagram Rank-Metric Codes

2 The Etzion-Silberstein (ES) Conjecture

- A Singleton Bound and the Conjecture
- An Illustrative Example: Triangular Diagrams

3 Recent Results on the ES Conjecture

A Modular Approach

Main Theorem (N., Stanojkovski, 2023)

If (\mathcal{D}, r) is MDS-constructible and $|\mathbb{P}| \ge \max_i |\mathcal{D} \cap \Delta_i^p| = 1$, then

$$\kappa_{\mathbb{F}}(\mathcal{D}, r) = \nu_{\min}(\mathcal{D}, r).$$

Main Theorem (N., Stanojkovski, 2023)

If (\mathcal{D}, r) is MDS-constructible and $|\mathbb{P}| \ge \max_{r} |\mathcal{D} \cap \Delta_{r}^{p}| = 1$, then

$$\kappa_{\mathbb{F}}(\mathcal{D}, r) = \nu_{\min}(\mathcal{D}, r).$$

Main steps:

1. **Theorem 1**. If the conjecture is true for $\mathcal{T}_n = (1, 2, ..., n)$, then it is also true for every MDS-constructible pair. combinatorial argument

Main Theorem (N., Stanojkovski, 2023)

If (\mathcal{D}, r) is MDS-constructible and $|\mathbb{P}| \ge \max_{i} |\mathcal{D} \cap \Delta_{i}^{p}| = 1$, then

$$\kappa_{\mathbb{F}}(\mathcal{D}, r) = \nu_{\min}(\mathcal{D}, r).$$

- 1. <u>Theorem 1</u>. If the conjecture is true for $\mathcal{T}_n = (1, 2, ..., n)$, then it is also true for every MDS-constructible pair. combinatorial argument
- 2. **Theorem 2.** The conjecture holds true for strictly monotone Ferrers diagrams of order $n = p^m$ in characteristic *p*. **algebraic argument**

Main Theorem (N., Stanojkovski, 2023)

If (\mathcal{D}, r) is MDS-constructible and $|\mathbb{P}| \ge \max_{r} |\mathcal{D} \cap \Delta_{r}^{p}| = 1$, then

$$\kappa_{\mathbb{F}}(\mathcal{D}, r) = \nu_{\min}(\mathcal{D}, r).$$

- 1. <u>Theorem 1</u>. If the conjecture is true for $\mathcal{T}_n = (1, 2, ..., n)$, then it is also true for every MDS-constructible pair. combinatorial argument
- 2. **Theorem 2.** The conjecture holds true for strictly monotone Ferrers diagrams of order $n = p^m$ in characteristic *p*. **algebraic argument**
- 3. **Lemmino.** If $\mathcal{D} = (c_1, \ldots, c_n)$ is strictly monotone of order *n*, then $\mathcal{D}' = (0, c_1, \ldots, c_n)$ is strictly monotone of order n + 1.

Main Theorem (N., Stanojkovski, 2023)

If (\mathcal{D}, r) is MDS-constructible and $|\mathbb{P}| \ge \max_{r} |\mathcal{D} \cap \Delta_{r}^{p}| = 1$, then

$$\kappa_{\mathbb{F}}(\mathcal{D}, r) = \nu_{\min}(\mathcal{D}, r).$$

- 1. <u>Theorem 1</u>. If the conjecture is true for $\mathcal{T}_n = (1, 2, ..., n)$, then it is also true for every MDS-constructible pair. combinatorial argument
- 2. **Theorem 2.** The conjecture holds true for strictly monotone Ferrers diagrams of order $n = p^m$ in characteristic *p*. **algebraic argument**
- 3. **Lemmino.** If $\mathcal{D} = (c_1, \ldots, c_n)$ is strictly monotone of order *n*, then $\mathcal{D}' = (0, c_1, \ldots, c_n)$ is strictly monotone of order n + 1.
- 4. T_n is strictly monotone.

Main Theorem (N., Stanojkovski, 2023)

If (\mathcal{D}, r) is MDS-constructible and $|\mathbb{P}| \ge \max_{i} |\mathcal{D} \cap \Delta_{i}^{p}| = 1$, then

$$\kappa_{\mathbb{F}}(\mathcal{D}, r) = \nu_{\min}(\mathcal{D}, r).$$

- 1. **Theorem 1**. If the conjecture is true for $T_n = (1, 2, ..., n)$, then it is also true for every MDS-constructible pair. combinatorial argument
- 2. **Theorem 2.** The conjecture holds true for strictly monotone Ferrers diagrams of order $n = p^m$ in characteristic *p*. **algebraic argument**
- 3. **Lemmino.** If $\mathcal{D} = (c_1, \ldots, c_n)$ is strictly monotone of order *n*, then $\mathcal{D}' = (0, c_1, \ldots, c_n)$ is strictly monotone of order n + 1.
- 4. T_n is strictly monotone.
- 5. If *n* not a power of *p*, then use Lemmino *h* times with $n + h = p^m$.

Main Theorem (N., Stanojkovski, 2023)

If (\mathcal{D}, r) is MDS-constructible, then

Main Theorem (N., Stanojkovski, 2023)

If (\mathcal{D}, r) is MDS-constructible, then

 $\kappa_{\mathbb{F}}(\mathcal{D}, r) = \nu_{\min}(\mathcal{D}, r).$

• Get rid of the field condition. Completely different construction!

Main Theorem (N., Stanojkovski, 2023)

If (\mathcal{D}, r) is MDS-constructible, then

- Get rid of the field condition. Completely different construction!
- First crucial idea: embed Ferrers diagrams matrix spaces in larger matrix spaces. (Lemmino)
- Second crucial idea: use **combinatorial properties** of MDS-constructible pairs. (Theorem 1)
- Third crucial idea: Use **flag** associated to **nilpotent endomorphism** σ id when $n = p^m$. (Theorem 2)

Main Theorem (N., Stanojkovski, 2023)

If (\mathcal{D}, r) is MDS-constructible, then

 $\kappa_{\mathbb{F}}(\mathcal{D}, r) = \nu_{\min}(\mathcal{D}, r).$

- Get rid of the field condition. Completely different construction!
- First crucial idea: embed Ferrers diagrams matrix spaces in larger matrix spaces. (Lemmino)
- Second crucial idea: use **combinatorial properties** of MDS-constructible pairs. (Theorem 1)
- Third crucial idea: Use **flag** associated to **nilpotent endomorphism** σ id when $n = p^m$. (Theorem 2)

Achtung: The ES Conjecture is still widely open

Alessandro Neri (UGent)

The End

Thank you! Dankjewel! Grazie!



Check out our preprint!

A. Neri. M. Stanojkovski. "A proof of the Etzion-Silberstein conjecture for monotone and MDS-constructible Ferrers diagrams", arXiv:2306.16407, 2023.





Main Theorem (N., Stanojkovski, 2023)

If (\mathcal{D}, r) is MDS-constructible, then

$$\kappa_{\mathbb{F}}(\mathcal{D}, r) = \nu_{\min}(\mathcal{D}, r).$$

- Get rid of the field condition. Completely different construction!
- First crucial idea: embed Ferrers diagrams matrix spaces in larger matrix spaces. (Lemmino)
- Second crucial idea: use **combinatorial properties** of MDS-constructible pairs. (Theorem 1)
- Third crucial idea: Use **flag** associated to **nilpotent endomorphism** σ id when $n = p^m$. (Theorem 2)

$$\mathbb{F}^{n \times n} \cong \bigoplus_{i=0}^{n-1} \mathbb{L} \cdot \sigma^i =: \mathbb{L}[\sigma].$$

$$\mathbb{F}^{n \times n} \cong \bigoplus_{i=0}^{n-1} \mathbb{L} \cdot \sigma^i =: \mathbb{L}[\sigma].$$

Idea

(1) Restrict it to $\mathbb{F}^{\mathcal{D}} \subseteq \mathbb{F}^{n \times n}$:

$$\mathbb{F}^{\mathcal{D}} \cong \mathbb{L}[\sigma; \mathcal{D}];$$

$$\mathbb{F}^{n \times n} \cong \bigoplus_{i=0}^{n-1} \mathbb{L} \cdot \sigma^i =: \mathbb{L}[\sigma].$$

Idea

(1) Restrict it to
$$\mathbb{F}^{\mathcal{D}} \subseteq \mathbb{F}^{n \times n}$$
:

$$\mathbb{F}^{\mathcal{D}} \cong \mathbb{L}[\sigma; \mathcal{D}];$$

(2) Use the Nullity-Degree Bound:

$$\mathbb{L}[\sigma; \mathcal{D}]_{n-r} = \{P(\sigma) \in \mathbb{L}[\sigma; \mathcal{D}] : \deg_{\sigma}(P) \leq n-r\};$$

$$\mathbb{F}^{n \times n} \cong_{\mathcal{B}} \bigoplus_{i=0}^{n-1} \mathbb{L} \cdot \sigma^i =: \mathbb{L}[\sigma].$$

Idea

(1) Restrict it to
$$\mathbb{F}^{\mathcal{D}} \subseteq \mathbb{F}^{n \times n}$$
:

$$\mathbb{F}^{\mathcal{D}} \cong_{\mathcal{B}} \mathbb{L}[\sigma; \mathcal{D}];$$

(2) Use the Nullity-Degree Bound:

$$\mathbb{L}[\sigma;\mathcal{D}]_{n-r} = \{P(\sigma) \in \mathbb{L}[\sigma;\mathcal{D}] : \deg_{\sigma}(P) \le n-r\};$$

(3) Hope that

$$\dim_{\mathbb{F}}(\mathbb{L}[\sigma;\mathcal{D}]_{n-r}) = \nu_{\min}(\mathcal{D},r).$$

$$\mathbb{F}^{n \times n} \cong_{\mathcal{B}} \bigoplus_{i=0}^{n-1} \mathbb{L} \cdot \sigma^i =: \mathbb{L}[\sigma].$$

Idea

(1) Restrict it to
$$\mathbb{F}^{\mathcal{D}} \subseteq \mathbb{F}^{n \times n}$$
:

$$\mathbb{F}^{\mathcal{D}} \cong_{\mathcal{B}} \mathbb{L}[\sigma; \mathcal{D}];$$

(2) Use the Nullity-Degree Bound:

$$\mathbb{L}[\sigma; \mathcal{D}]_{n-r} = \{P(\sigma) \in \mathbb{L}[\sigma; \mathcal{D}] : \deg_{\sigma}(P) \leq n-r\};$$

(3) Hope that

$$\dim_{\mathbb{F}}(\mathbb{L}[\sigma;\mathcal{D}]_{n-r}) = \nu_{\min}(\mathcal{D}, r).$$

Achtung: Need a smart choice of an \mathbb{F} -basis \mathcal{B} of \mathbb{L} !

Alessandro Neri (UGent)

$$p = \operatorname{char}(\mathbb{F}), \qquad n = p^m.$$

$$\bar{\sigma} := \sigma - \mathrm{id}, \qquad \qquad \mathcal{F}_i := \mathrm{ker}(\bar{\sigma}^i).$$

$$p = \operatorname{char}(\mathbb{F}), \qquad n = p^m.$$

$$\bar{\sigma} := \sigma - \mathrm{id}, \qquad \qquad \mathcal{F}_i := \mathrm{ker}(\bar{\sigma}^i).$$

• $\bar{\sigma}$ is nilpotent of order *n*.

$$p = \operatorname{char}(\mathbb{F}), \qquad n = p^m.$$

$$\bar{\sigma} := \sigma - \mathrm{id}, \qquad \qquad \mathcal{F}_i := \mathrm{ker}(\bar{\sigma}^i).$$

- $\bar{\sigma}$ is nilpotent of order *n*.
- For each $i \in \{0, ..., n-1\}$, one has $\deg_{\sigma}(\bar{\sigma}^i) = i$. (DEG)

$$p = \operatorname{char}(\mathbb{F}), \qquad n = p^m.$$

$$\bar{\sigma} := \sigma - \mathrm{id}, \qquad \qquad \mathcal{F}_i := \mathrm{ker}(\bar{\sigma}^i).$$

- $\bar{\sigma}$ is nilpotent of order *n*.
- For each $i \in \{0, \dots, n-1\}$, one has $\deg_{\sigma}(\bar{\sigma}^i) = i$.
- $(\bar{\sigma}^i : i \in \{0, \dots, n-1\})$ is an \mathbb{L} -basis of $\mathbb{L}[\sigma]$.

(DEG)
$$p = \operatorname{char}(\mathbb{F}), \qquad n = p^m.$$

$$\bar{\sigma} := \sigma - \mathrm{id}, \qquad \qquad \mathcal{F}_i := \mathrm{ker}(\bar{\sigma}^i).$$

• $\bar{\sigma}$ is nilpotent of order *n*.

• For each
$$i \in \{0, ..., n-1\}$$
, one has $\deg_{\sigma}(\bar{\sigma}^i) = i$.

- $(\bar{\sigma}^i : i \in \{0, \dots, n-1\})$ is an \mathbb{L} -basis of $\mathbb{L}[\sigma]$.
- For each $i \in \{0, \ldots, n\}$, one has $\dim_{\mathbb{F}} \mathcal{F}_i = i$.

(DEG)

$$p = \operatorname{char}(\mathbb{F}), \qquad n = p^m.$$

$$\bar{\sigma} := \sigma - \mathrm{id}, \qquad \qquad \mathcal{F}_i := \mathrm{ker}(\bar{\sigma}^i).$$

• $\bar{\sigma}$ is nilpotent of order *n*.

• For each
$$i \in \{0, \dots, n-1\}$$
, one has $\deg_{\sigma}(\bar{\sigma}^i) = i$.

- $(\bar{\sigma}^i : i \in \{0, \dots, n-1\})$ is an \mathbb{L} -basis of $\mathbb{L}[\sigma]$.
- For each $i \in \{0, \ldots, n\}$, one has dim_F $\mathcal{F}_i = i$.
- For each $i \in \{1, \ldots, n\}$, one has $\mathcal{F}_{i-1} \subset \mathcal{F}_i$.

(DEG)

$$p = \operatorname{char}(\mathbb{F}), \qquad n = p^m.$$

$$\bar{\sigma} := \sigma - \mathrm{id}, \qquad \qquad \mathcal{F}_i := \mathrm{ker}(\bar{\sigma}^i).$$

• $\bar{\sigma}$ is nilpotent of order *n*.

• For each
$$i \in \{0, \dots, n-1\}$$
, one has $\deg_{\sigma}(\bar{\sigma}^i) = i$.

- $(\bar{\sigma}^i : i \in \{0, \dots, n-1\})$ is an \mathbb{L} -basis of $\mathbb{L}[\sigma]$.
- For each $i \in \{0, \ldots, n\}$, one has dim_{\mathbb{F}} $\mathcal{F}_i = i$.
- For each $i \in \{1, \ldots, n\}$, one has $\mathcal{F}_{i-1} \subset \mathcal{F}_i$.
- For every i, j with $i + j \le n$, one has $\mathcal{F}_i \cdot \mathcal{F}_j \subseteq \mathcal{F}_{i+j-1}$. (ABS)

(DEG)

$$p = \operatorname{char}(\mathbb{F}), \qquad n = p^m.$$

$$\bar{\sigma} := \sigma - \mathrm{id}, \qquad \qquad \mathcal{F}_i := \mathrm{ker}(\bar{\sigma}^i).$$

• $\bar{\sigma}$ is nilpotent of order *n*.

• For each
$$i \in \{0, \dots, n-1\}$$
, one has $\deg_{\sigma}(\bar{\sigma}^i) = i$. (DEG)

- $(\bar{\sigma}^i : i \in \{0, \dots, n-1\})$ is an \mathbb{L} -basis of $\mathbb{L}[\sigma]$.
- For each $i \in \{0, \ldots, n\}$, one has dim_F $\mathcal{F}_i = i$.
- For each $i \in \{1, \ldots, n\}$, one has $\mathcal{F}_{i-1} \subset \mathcal{F}_i$.
- For every i, j with $i + j \le n$, one has $\mathcal{F}_i \cdot \mathcal{F}_j \subseteq \mathcal{F}_{i+j-1}$. (ABS)

$$\mathcal{F}:=(\mathcal{F}_0,\mathcal{F}_1,\ldots,\mathcal{F}_n)$$
 full \mathbb{F} -flag

$$p = \operatorname{char}(\mathbb{F}), \qquad n = p^m.$$

$$\bar{\sigma} := \sigma - \mathrm{id}, \qquad \qquad \mathcal{F}_i := \mathrm{ker}(\bar{\sigma}^i).$$

• $\bar{\sigma}$ is nilpotent of order *n*.

• For each
$$i \in \{0, \dots, n-1\}$$
, one has $\deg_{\sigma}(\bar{\sigma}^i) = i$. (DEG)

- $(\bar{\sigma}^i : i \in \{0, \dots, n-1\})$ is an \mathbb{L} -basis of $\mathbb{L}[\sigma]$.
- For each $i \in \{0, \ldots, n\}$, one has dim_F $\mathcal{F}_i = i$.
- For each $i \in \{1, \ldots, n\}$, one has $\mathcal{F}_{i-1} \subset \mathcal{F}_i$.
- For every i, j with $i + j \le n$, one has $\mathcal{F}_i \cdot \mathcal{F}_j \subseteq \mathcal{F}_{i+j-1}$. (ABS)

$$\mathcal{F} := (\mathcal{F}_0, \mathcal{F}_1, \dots, \mathcal{F}_n)$$
 full \mathbb{F} -flag

Smart choice: $\mathcal{B} = (\beta_1, \ldots, \beta_n)$ compatible with $\mathcal{F}: \langle \beta_1, \ldots, \beta_i \rangle_{\mathbb{F}} = \mathcal{F}_i$.

Restricted Skew Algebra Isomorphism

Strictly monotone Ferrers Diagram:

 $\mathcal{D} = (c_1, \ldots, c_n)$ if it satisfies

 $c_i > 0$ implies $c_{i+1} > c_i$.

Restricted Skew Algebra Isomorphism

Strictly monotone Ferrers Diagram: $\mathcal{D} = (c_1, \ldots, c_n)$ if it satisfies

 $c_i > 0$ implies $c_{i+1} > c_i$.



Restricted Skew Algebra Isomorphism



 $c_i > 0$ implies $c_{i+1} > c_i$.



Theorem (N., Stanojkovski, 2023)

Let $\mathcal{D} = (c_1, ..., c_n)$ be a **strictly monotone** Ferrers diagram of order $n = p^m$. Then for any \mathcal{F} -compatible basis \mathcal{B} of \mathbb{L} we have

$$\mathbb{F}^{\mathcal{D}} \cong_{\mathcal{B}} \mathbb{L}[\sigma; \mathcal{D}] = \bigoplus_{i=1}^{n} \mathcal{F}_{c_{i}} \bar{\sigma}^{i-1} = \left\{ \sum_{i=1}^{n} \lambda_{i} \bar{\sigma}^{i-1} : \lambda_{i} \in \mathcal{F}_{c_{i}} \right\}.$$

Maximal Ferrers Diagrams Codes

Theorem (N., Stanojkovski, 2023)

Let $\mathcal{D} = (c_1, \ldots, c_n)$ be a **strictly monotone** Ferrers diagram of order $n = p^m$. Then, for every $d \in \{2, \ldots, n\}$,

$$\mathbb{L}[\sigma; \mathcal{D}]_{n-r} = \{P(\sigma) \in \mathbb{L}[\sigma; \mathcal{D}] : \deg_{\sigma}(P) \leq n-r\}$$

is a $[\mathcal{D}, \nu_{\min}(\mathcal{D}, r), r]_{\mathbb{F}}$ code.

Maximal Ferrers Diagrams Codes

Theorem (N., Stanojkovski, 2023)

Let $\mathcal{D} = (c_1, \ldots, c_n)$ be a **strictly monotone** Ferrers diagram of order $n = p^m$. Then, for every $d \in \{2, \ldots, n\}$,

$$\mathbb{L}[\sigma; \mathcal{D}]_{n-r} = \{P(\sigma) \in \mathbb{L}[\sigma; \mathcal{D}] : \deg_{\sigma}(P) \leq n-r\}$$

is a $[\mathcal{D}, \nu_{\min}(\mathcal{D}, r), r]_{\mathbb{F}}$ code.

• Nullity-Degree bound: $rk(A) \ge r$;

Maximal Ferrers Diagrams Codes

Theorem (N., Stanojkovski, 2023)

Let $\mathcal{D} = (c_1, \ldots, c_n)$ be a **strictly monotone** Ferrers diagram of order $n = p^m$. Then, for every $d \in \{2, \ldots, n\}$,

$$\mathbb{L}[\sigma; \mathcal{D}]_{n-r} = \{P(\sigma) \in \mathbb{L}[\sigma; \mathcal{D}] : \deg_{\sigma}(P) \leq n-r\}$$

is a $[\mathcal{D}, \nu_{\min}(\mathcal{D}, r), r]_{\mathbb{F}}$ code.

- Nullity-Degree bound: $rk(A) \ge r$;
- dim_{\mathbb{F}}($\mathbb{L}[\sigma; \mathcal{D}]_{n-r}$) = $c_1 + c_2 + \ldots + c_{n-r} = \nu_{r-1}(\mathcal{D}, r) = \nu_{\min}(\mathcal{D}, r)$.

•
$$\mathbb{F} = \mathbb{F}_2$$
. $n = 6$, $r = 4$, $\mathcal{D} = \mathcal{T}_6$.

• $\nu_{\min}(\mathcal{D}, 4) = 6.$



- $\mathbb{F} = \mathbb{F}_2$. n = 6, r = 4, $\mathcal{D} = \mathcal{T}_6$.
- $\nu_{\min}(\mathcal{D}, 4) = 6.$
- Use Lemmino 2 times: $\mathcal{D} \to \mathcal{D}'$.



- $\mathbb{F} = \mathbb{F}_2$. n = 6, r = 4, $\mathcal{D} = \mathcal{T}_6$.
- $\nu_{\min}(\mathcal{D}, 4) = 6.$
- Use Lemmino 2 times: $\mathcal{D} \to \mathcal{D}'$.
- $\mathbb{L} = \mathbb{F}_{2^8} = \mathbb{F}_2(\gamma)$, with $\gamma^8 + \gamma^4 + \gamma^3 + \gamma^2 + 1 = 0$.



- $\mathbb{F} = \mathbb{F}_2$, n = 6, r = 4, $\mathcal{D} = \mathcal{T}_6$.
- $\nu_{\min}(\mathcal{D}, 4) = 6.$
- Use Lemmino 2 times: $\mathcal{D} \to \mathcal{D}'$.
- $\mathbb{L} = \mathbb{F}_{2^8} = \mathbb{F}_2(\gamma)$, with $\gamma^8 + \gamma^4 + \gamma^3 + \gamma^2 + 1 = 0$. • $\sigma: \mathcal{B} \mapsto \mathcal{B}^2$.
- $\bar{\sigma} = \sigma \mathrm{id}$
- $\mathcal{F}_i = \ker(\bar{\sigma}^i), \quad \mathcal{F} = (\mathcal{F}_0, \dots, \mathcal{F}_8).$
- $\mathcal{B} = (1, \gamma^{170}, \gamma^{136}, \gamma^{204}, \gamma^{222}, \gamma^{38}, \gamma^{143}, \gamma^5)$ is \mathcal{F} -compatible.



- $\mathbb{F} = \mathbb{F}_2$. n = 6, r = 4, $\mathcal{D} = \mathcal{T}_6$.
- $\nu_{\min}(\mathcal{D}, 4) = 6.$
- Use Lemmino 2 times: $\mathcal{D} \to \mathcal{D}'$.
- $\mathbb{L} = \mathbb{F}_{2^8} = \mathbb{F}_2(\gamma)$, with $\gamma^8 + \gamma^4 + \gamma^3 + \gamma^2 + 1 = 0$. • $\sigma : \beta \mapsto \beta^2$.
- $\bar{\sigma} = \sigma \mathrm{id}.$
- $\mathcal{F}_i = \ker(\bar{\sigma}^i), \quad \mathcal{F} = (\mathcal{F}_0, \dots, \mathcal{F}_8).$
- $\mathcal{B} = (1, \gamma^{170}, \gamma^{136}, \gamma^{204}, \gamma^{222}, \gamma^{38}, \gamma^{143}, \gamma^5)$ is \mathcal{F} -compatible.

$$\mathbb{F}^{\mathcal{D}} \cong \mathbb{F}_{2^{\aleph}}[\sigma; \mathcal{D}'] = \bigoplus_{i=3}^{\aleph} \mathcal{F}_{i-2} \bar{\sigma}^{i-1}.$$



- $\mathbb{F} = \mathbb{F}_2$. n = 6, r = 4, $\mathcal{D} = \mathcal{T}_6$.
- $\nu_{\min}(\mathcal{D}, 4) = 6.$
- Use Lemmino 2 times: $\mathcal{D} \to \mathcal{D}'$.
- $\mathbb{L} = \mathbb{F}_{2^8} = \mathbb{F}_2(\gamma)$, with $\gamma^8 + \gamma^4 + \gamma^3 + \gamma^2 + 1 = 0$. • $\sigma : \beta \mapsto \beta^2$.
- $\bar{\sigma} = \sigma \mathrm{id}$.
- $\mathcal{F}_i = \ker(\bar{\sigma}^i), \quad \mathcal{F} = (\mathcal{F}_0, \dots, \mathcal{F}_8).$
- $\mathcal{B} = (1, \gamma^{170}, \gamma^{136}, \gamma^{204}, \gamma^{222}, \gamma^{38}, \gamma^{143}, \gamma^5)$ is \mathcal{F} -compatible.

$$\mathbb{F}^{\mathcal{D}} \cong \mathbb{F}_{2^8}[\sigma; \mathcal{D}'] = \bigoplus_{i=3}^8 \mathcal{F}_{i-2}\bar{\sigma}^{i-1}.$$

The $[\mathcal{D}', 6, 4]_{\mathbb{F}_2}$ code representation in $\mathbb{F}_{2^8}[\sigma; \mathcal{D}']$ is $\mathbb{F}_{2^8}[\sigma; \mathcal{D}']_4 = \langle \bar{\sigma}^2, \bar{\sigma}^3, \gamma^{170} \bar{\sigma}^3, \bar{\sigma}^4, \gamma^{170} \bar{\sigma}^4, \gamma^{136} \bar{\sigma}^4 \rangle_{\mathbb{F}_2}.$



$ \left(\begin{array}{c} 0\\0\\0\\0\\0\\0\\0\\0\\0\\0\end{array}\right) $	0 0 0 0 0 0 0	1 0 0 0 0 0 0	0 1 0 0 0 0 0	0 0 1 0 0 0 0 0	0 0 1 0 0 0 0	0 0 0 1 0 0 0	0 0 0 0 1 0 0) ,	$ \left(\begin{array}{c} 0\\ 0\\ 0\\ 0\\ 0\\ 0\\ 0\\ 0\\ 0\\ 0 \end{array}\right) $	0 0 0 0 0 0 0	0 0 0 0 0 0 0	1 0 0 0 0 0 0	0 1 0 0 0 0 0 0	0 1 0 0 0 0 0	0 0 1 0 0 0 0	0 0 0 1 0 0 0	,	$ \left(\begin{array}{c} 0\\ 0\\ 0\\ 0\\ 0\\ 0\\ 0\\ 0\\ 0\\ 0 \end{array}\right) $	0 0 0 0 0 0 0	0 0 0 0 0 0 0	0 1 0 0 0 0 0 0	1 0 0 0 0 0 0	0 1 0 1 0 0 0 0	1 0 1 0 0 0 0	0) 1 0 1 0 1 0 0
$ \left(\begin{array}{c} 0\\0\\0\\0\\0\\0\\0\\0\\0\\0\end{array}\right) $	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0	0 0 0 0 0 0 0	1 0 0 0 0 0 0	0 1 0 0 0 0 0	0 0 1 0 0 0 0 0	0 0 1 0 0 0 0	,	$ \left(\begin{array}{c} 0\\0\\0\\0\\0\\0\\0\\0\\0\\0\end{array}\right) $	0 0 0 0 0 0 0 0	0 0 0 0 0 0 0	0 0 0 0 0 0 0 0 0	0 1 0 0 0 0 0 0	1 1 0 0 0 0 0 0 0	0 1 0 1 0 0 0 0	1 1 1 0 0 0	,	$ \left(\begin{array}{c} 0\\ 0\\ 0\\ 0\\ 0\\ 0\\ 0\\ 0\\ 0\\ 0 \end{array}\right) $	0 0 0 0 0 0 0	0 0 0 0 0 0 0	0 0 0 0 0 0 0	0 1 0 0 0 0	0 1 0 1 0 0 0 0	0 1 0 0 0 0 0	1 1 0 0 0 0 0

,

(1 0 0 0 0 0	0 1 0 0 0	0 0 1 0 0	0 0 1 0 0	0 0 0 1 0	0 0 0 0 1	,	0 0 0 0 0 0	1 0 0 0 0	0 1 0 0 0	0 0 1 0 0	0 0 1 0	0 0 0 1 0),	$ \left(\begin{array}{c} 0\\ 0\\ 0\\ 0\\ 0\\ 0\\ 0\\ 0 \end{array}\right) $	0 1 0 0 0	1 1 0 0 0	0 1 0 1 0 0	1 0 1 1 0 0	0 1 0 1 0 1 1	
(0 0 0 0 0 0 0 0	0 0 0 0 0	1 0 0 0 0	0 1 0 0 0	0 0 1 0 0	0 0 1 0 0	,	$ \left(\begin{array}{c} 0\\ 0\\ 0\\ 0\\ 0\\ 0\\ 0 \end{array}\right) $	0 0 0 0 0	0 1 0 0 0	1 1 0 0 0	0 1 0 1 0	1 0 1 1 0 0),	$ \left(\begin{array}{c} 0\\ 0\\ 0\\ 0\\ 0\\ 0\\ 0 \end{array}\right) $	0 0 0 0 0	0 0 1 0 0	0 1 0 1 0 0	0 1 1 0 0	1 1 0 0 0 0	

,