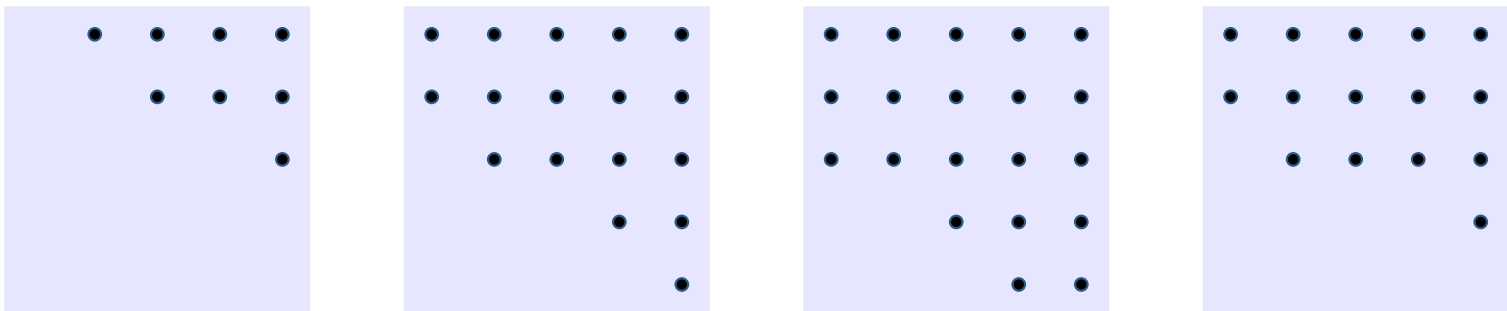
Ferrers diagram rank-metric codes and a conjecture of Etzion and Silberstein

Mima Stanojkovski, Università di Trento

JOINT WORK WITH **Alessandro Neri, Università di Napoli**



Second UMI Meeting for Doctoral Students

Napoli, 14. June 2024

Let $\mathcal{M} = (X, \mathrm{dist})$ be a metric space.

Definition. A **code** in $\mathcal{M}$ is a subset $\mathcal{C}$ of cardinality at least 2.

Let $\mathcal{M} = (X, \mathrm{dist})$ be a metric space.

Definition. A **code** in $\mathcal{M}$ is a subset $\mathcal{C}$ of cardinality at least 2. If $\mathcal{C}$ is finite, the **minimum distance** of $\mathcal{C}$ is

$$d(\mathcal{C}) = \min\{\mathrm{dist}(x, y) : x, y \in \mathcal{C},\ x \neq y\}.$$

Let $\mathcal{M} = (X, \mathrm{dist})$ be a metric space.

Definition. A **code** in $\mathcal{M}$ is a subset $\mathcal{C}$ of cardinality at least 2. If $\mathcal{C}$ is finite, the **minimum distance** of $\mathcal{C}$ is

$$d(\mathcal{C}) = \min\{\mathrm{dist}(x, y) : x, y \in \mathcal{C},\ x \neq y\}.$$

Example. Examples of metric spaces used for applications are:

- $\mathcal{M} = (\mathbb{R}^n, \mathrm{dist})$ with $\mathrm{dist}(a, b) = |a - b|$

  Euclidean metric

Let $\mathcal{M} = (X, \mathrm{dist})$ be a metric space.

Definition. A **code** in $\mathcal{M}$ is a subset $\mathcal{C}$ of cardinality at least 2. If $\mathcal{C}$ is finite, the **minimum distance** of $\mathcal{C}$ is

$$d(\mathcal{C}) = \min\{\mathrm{dist}(x, y) : x, y \in \mathcal{C},\ x \neq y\}.$$

Example. Examples of metric spaces used for applications are:

- $\mathcal{M} = (\mathbb{R}^n, \mathrm{dist})$ with $\mathrm{dist}(a, b) = |a - b|$

  Euclidean metric

- $\mathcal{M} = (\mathbb{F}_q^n, \mathrm{dist})$ with $\mathrm{dist}(v, w) = \#\{i : v_i \neq w_i\}$

  Hamming metric

Let $\mathcal{M} = (X, \mathrm{dist})$ be a metric space.

Definition. A **code** in $\mathcal{M}$ is a subset $\mathcal{C}$ of cardinality at least 2. If $\mathcal{C}$ is finite, the **minimum distance** of $\mathcal{C}$ is

$$d(\mathcal{C}) = \min\{\mathrm{dist}(x, y) : x, y \in \mathcal{C},\ x \neq y\}.$$

Example. Examples of metric spaces used for applications are:

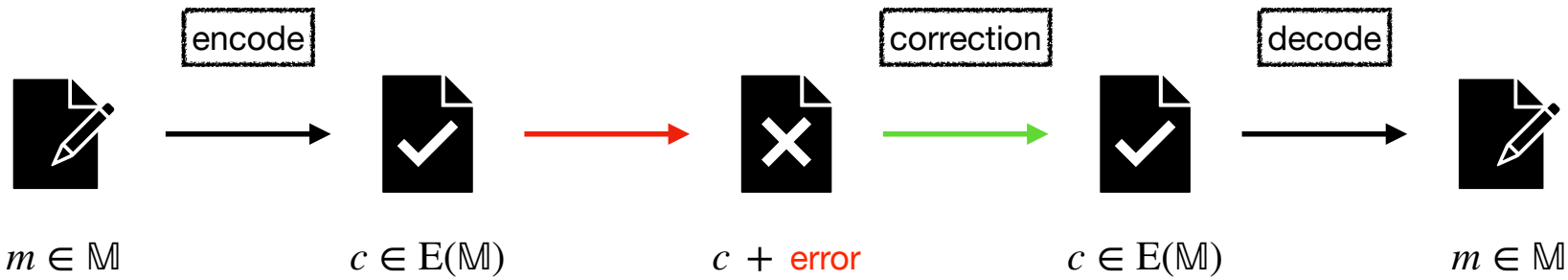
- $\mathcal{M} = (\mathbb{R}^n, \mathrm{dist})$ with $\mathrm{dist}(a, b) = |a - b|$

  Euclidean metric
- $\mathcal{M} = (\mathbb{F}_q^n, \mathrm{dist})$ with $\mathrm{dist}(v, w) = \#\{i : v_i \neq w_i\}$

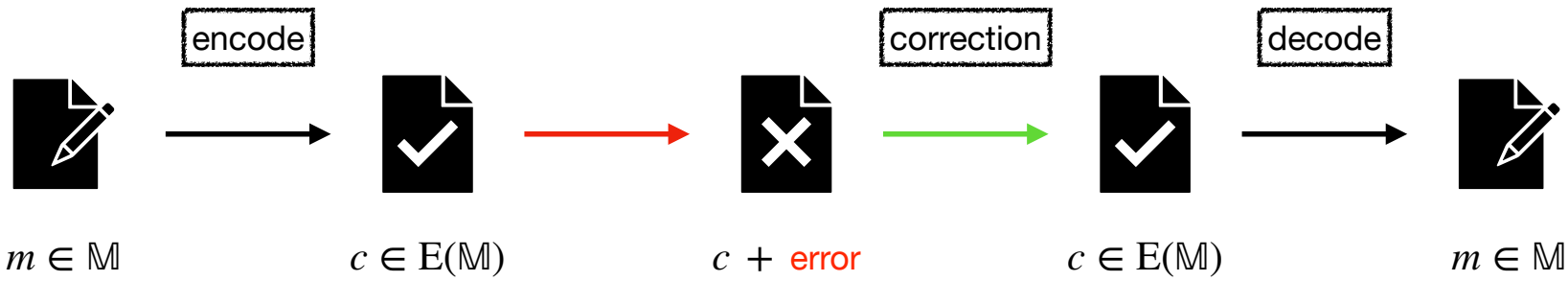
  Hamming metric
- $\mathcal{M} = (\mathbb{F}_q^{m \times n}, \mathrm{dist})$ with $\mathrm{dist}(A, B) = \mathrm{rk}(A - B)$

  Rank metric

Transmitting a message through a possibly noisy channel:



Transmitting a message through a possibly noisy channel:



We can interpret the situation as follows:

- $\mathbb{M}$ is a finite set – space of messages
- $\mathrm{E} : \mathbb{M} \to \mathbb{A}^n$ is an injective map – encoding map
  where $\mathbb{A}$ is a finite alphabet and $n \in \mathbb{Z}_{>0}$ is called length
- $\mathcal{C} = \mathrm{E}(\mathbb{M})$ is the code

. . . what do we need the length and distance for?

. . . what do we need the length and distance for?

Example. If $\mathbb{M} = \{\text{no, yes}\}$ and $\mathcal{C} = \{0, 1\} \subseteq \mathbb{F}_2^1$, then we are pretty much hopeless for what concerns the correction of errors: we can't tell $c = 0$ apart from $c' = 1$.

. . . what do we need the length and distance for?

Example. If $\mathbb{M} = \{\text{no, yes}\}$ and $\mathcal{C} = \{0, 1\} \subseteq \mathbb{F}_2^1$, then we are pretty much hopeless for what concerns the correction of errors: we can't tell $c = 0$ apart from $c' = 1$.

First solution: add redundancy through $n \rightsquigarrow \mathcal{C} = \{0^n, 1^n\} \subseteq \mathbb{F}_2^n$

. . . what do we need the length and distance for?

Example. If $\mathbb{M} = \{\text{no, yes}\}$ and $\mathcal{C} = \{0, 1\} \subseteq \mathbb{F}_2^1$, then we are pretty much hopeless for what concerns the correction of errors: we can't tell $c = 0$ apart from $c' = 1$.

First solution: add redundancy through $n \rightsquigarrow \mathcal{C} = \{0^n, 1^n\} \subseteq \mathbb{F}_2^n$

Remark. We could have chosen a different encryption of $\mathbb{M}$, but this one maximizes the minimum distance!

. . . what do we need the length and distance for?

Example. If $\mathbb{M} = \{\text{no, yes}\}$ and $\mathcal{C} = \{0, 1\} \subseteq \mathbb{F}_2^1$, then we are pretty much hopeless for what concerns the correction of errors: we can't tell $c = 0$ apart from $c' = 1$.

First solution: add redundancy through $n \rightsquigarrow \mathcal{C} = \{0^n, 1^n\} \subseteq \mathbb{F}_2^n$

Remark. We could have chosen a different encryption of $\mathbb{M}$, but this one maximizes the minimum distance!

Example. If $n = 6$ and $\tilde{c} = (0, 0, 1, 0, 0, 1) \in \mathbb{F}_2^6$ is transmitted, then it is easier to recover c if

$$\mathcal{C} = \{(0, 0, 0, 0, 0, 0), (1, 1, 1, 1, 1, 1)\}$$

than if we worked with

$$\mathcal{C}' = \{(0, 0, 0, 0, 0, 1), (0, 0, 1, 0, 0, 0)\}.$$

In summary, we want that

- the length is sufficiently large, but also not too large (for efficiency in transmission)
- the minimum distance of the code is large (so we can correct errors).

In summary, we want that

- the length is sufficiently large, but also not too large (for efficiency in transmission)
- the minimum distance of the code is large (so we can correct errors).

Theorem (Singleton bound). If $\mathcal{C} \subseteq \mathbb{F}_q^n$ is considered with the Hamming metric, then

$$|\mathcal{C}| \leq q^{n-d(\mathcal{C})+1}.$$

In summary, we want that

- the length is sufficiently large, but also not too large (for efficiency in transmission)
- the minimum distance of the code is large (so we can correct errors).

Theorem (Singleton bound). If $\mathcal{C} \subseteq \mathbb{F}_q^n$ is considered with the Hamming metric, then

$$|\mathcal{C}| \leq q^{n-d(\mathcal{C})+1}.$$

Remark. In order to have an efficient performance (storage, encoding, decoding, ...), adding more structure might be beneficial.

Definition. A code $\mathcal{C}$ in $\mathcal{M} = (X, \mathrm{dist})$ is called **linear** if X is a vector space over some field $\mathbb{F}$ and $\mathcal{C}$ is an $\mathbb{F}$-subspace of X.

Definition. A code $\mathcal{C}$ in $\mathcal{M} = (X, \mathrm{dist})$ is called **linear** if X is a vector space over some field $\mathbb{F}$ and $\mathcal{C}$ is an $\mathbb{F}$-subspace of X.

Remark. If $\mathcal{C}$ is a linear code, then

$$d(\mathcal{C}) = \min\{\mathrm{dist}(x, 0) : x \in \mathcal{C} \setminus \{0\}\}$$

Definition. A code $\mathcal{C}$ in $\mathcal{M} = (X, \mathrm{dist})$ is called **linear** if X is a vector space over some field $\mathbb{F}$ and $\mathcal{C}$ is an $\mathbb{F}$-subspace of X.

Remark. If $\mathcal{C}$ is a linear code, then

$$d(\mathcal{C}) = \min\{\mathrm{dist}(x, 0) : x \in \mathcal{C} \setminus \{0\}\}$$

so going back to our original examples:

- $d(\mathcal{C}) = \min\{|x| : x \in \mathcal{C} \subset \mathbb{R}^n, x \neq 0\}$ Euclidean metric

Definition. A code $\mathcal{C}$ in $\mathcal{M} = (X, \mathrm{dist})$ is called **linear** if X is a vector space over some field $\mathbb{F}$ and $\mathcal{C}$ is an $\mathbb{F}$-subspace of X.

Remark. If $\mathcal{C}$ is a linear code, then

$$d(\mathcal{C}) = \min\{\mathrm{dist}(x, 0) : x \in \mathcal{C} \setminus \{0\}\}$$

so going back to our original examples:

- $d(\mathcal{C}) = \min\{|x| : x \in \mathcal{C} \subset \mathbb{R}^n, x \neq 0\}$ Euclidean metric
- $d(\mathcal{C}) = \min\{\#\mathrm{supp}(v) : v \in \mathcal{C} \subset \mathbb{F}_q^n, v \neq 0\}$ Hamming metric

  Singleton bound: $\dim \mathcal{C} \leq n - d(\mathcal{C}) + 1$

Definition. A code $\mathcal{C}$ in $\mathcal{M} = (X, \mathrm{dist})$ is called **linear** if X is a vector space over some field $\mathbb{F}$ and $\mathcal{C}$ is an $\mathbb{F}$-subspace of X.

Remark. If $\mathcal{C}$ is a linear code, then

$$d(\mathcal{C}) = \min\{\mathrm{dist}(x, 0) : x \in \mathcal{C} \setminus \{0\}\}$$

so going back to our original examples:

- $d(\mathcal{C}) = \min\{|x| : x \in \mathcal{C} \subset \mathbb{R}^n, x \neq 0\}$ Euclidean metric
- $d(\mathcal{C}) = \min\{\#\mathrm{supp}(v) : v \in \mathcal{C} \subset \mathbb{F}_q^n, v \neq 0\}$ Hamming metric

  Singleton bound: $\dim \mathcal{C} \leq n - d(\mathcal{C}) + 1$
- $d(\mathcal{C}) = \min\{\mathrm{rk}(A) : A \in \mathcal{C} \subset \mathbb{F}_q^{m \times n}, A \neq 0\}$ Rank metric

Today we will focus on linear codes with the rank metric, also known as rank-metric codes.

Let $\mathbb{F}$ be a (finite) field and let d, k, m, n be positive integers.

Definition. An $[n \times m, k, d]_{\mathbb{F}}$ **rank-metric code** is a linear subspace $\mathcal{C}$ of $\mathbb{F}^{n \times m}$ of dimension k and such that

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

Let $\mathbb{F}$ be a (finite) field and let d, k, m, n be positive integers.

Definition. An $[n \times m, k, d]_{\mathbb{F}}$ **rank-metric code** is a linear subspace $\mathcal{C}$ of $\mathbb{F}^{n \times m}$ of dimension k and such that

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

Theorem (Singleton-like bound).

$$k \leq \min\{n(m - d + 1), m(n - d + 1)\}.$$

Let $\mathbb{F}$ be a (finite) field and let d, k, m, n be positive integers.

Definition. An $[n \times m, k, d]_{\mathbb{F}}$ **rank-metric code** is a linear subspace $\mathcal{C}$ of $\mathbb{F}^{n\times m}$ of dimension k and such that

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

Theorem (Singleton-like bound).

$$k \leq \min\{n(m-d+1), m(n-d+1)\}.$$

Proof. Let $\pi : \mathbb{F}^{n\times m} \cong \mathbb{F}^{n\times(d-1)} \times \mathbb{F}^{n\times(m-d+1)} \to \mathbb{F}^{n\times(m-d+1)}$.

Let $\mathbb{F}$ be a (finite) field and let d, k, m, n be positive integers.

Definition. An $[n \times m, k, d]_{\mathbb{F}}$ **rank-metric code** is a linear subspace $\mathcal{C}$ of $\mathbb{F}^{n\times m}$ of dimension k and such that

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

Theorem (Singleton-like bound).

$$k \leq \min\{n(m-d+1), m(n-d+1)\}.$$

Proof. Let $\pi : \mathbb{F}^{n\times m} \cong \mathbb{F}^{n\times(d-1)} \times \mathbb{F}^{n\times(m-d+1)} \to \mathbb{F}^{n\times(m-d+1)}$.
Then every $A \in \ker\pi$ satisfies $\mathrm{rk}(A) \leq d-1$: so $\ker\pi \cap \mathcal{C} = \{0\}$.

Let $\mathbb{F}$ be a (finite) field and let d, k, m, n be positive integers.

Definition. An $[n \times m, k, d]_{\mathbb{F}}$ **rank-metric code** is a linear subspace $\mathcal{C}$ of $\mathbb{F}^{n\times m}$ of dimension k and such that

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

Theorem (Singleton-like bound).

$$k \leq \min\{n(m-d+1), m(n-d+1)\}.$$

Proof. Let $\pi : \mathbb{F}^{n\times m} \cong \mathbb{F}^{n\times(d-1)} \times \mathbb{F}^{n\times(m-d+1)} \to \mathbb{F}^{n\times(m-d+1)}$.
Then every $A \in \ker\pi$ satisfies $\mathrm{rk}(A) \leq d-1$: so $\ker\pi \cap \mathcal{C} = \{0\}$.
In particular $\pi : \mathcal{C} \to \mathbb{F}^{n\times(m-d+1)}$ is injective. □

Let $\mathbb{F}$ be a (finite) field and let d, k, m, n be positive integers.

Definition. An $[n \times m, k, d]_{\mathbb{F}}$ **rank-metric code** is a linear subspace $\mathcal{C}$ of $\mathbb{F}^{n\times m}$ of dimension k and such that

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

Theorem (Singleton-like bound).

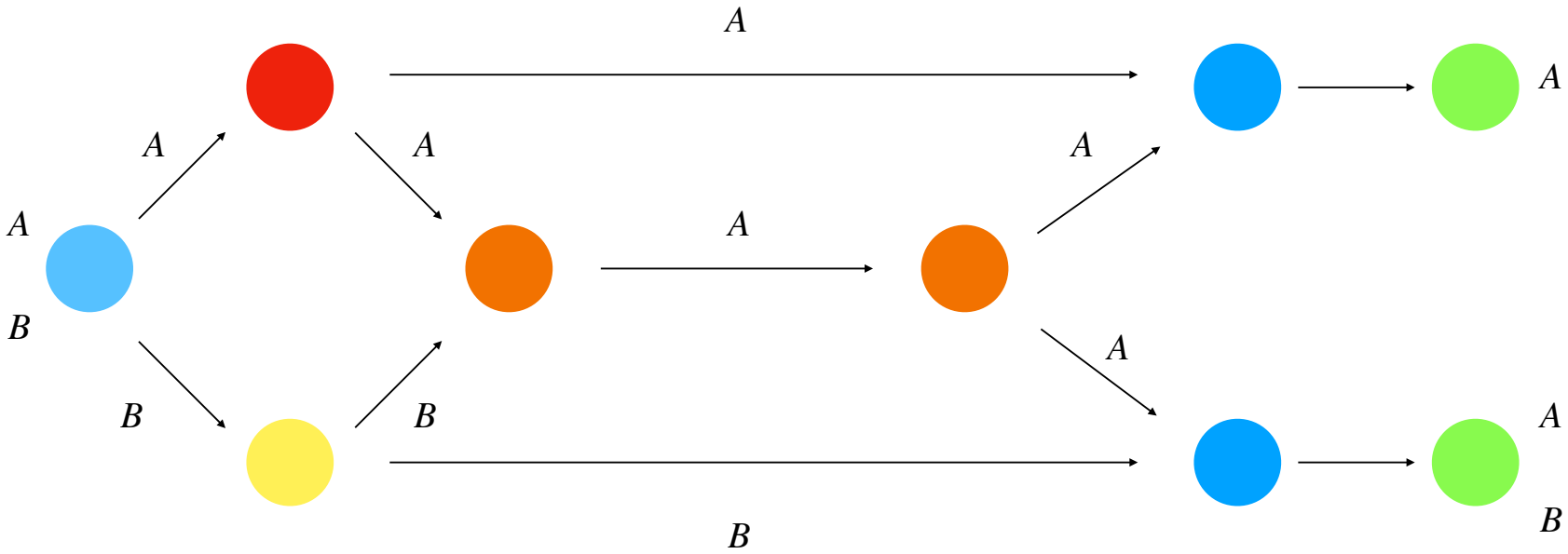
$$k \leq \min\{n(m-d+1), m(n-d+1)\}.$$

Proof. Let $\pi : \mathbb{F}^{n\times m} \cong \mathbb{F}^{n\times(d-1)} \times \mathbb{F}^{n\times(m-d+1)} \to \mathbb{F}^{n\times(m-d+1)}$.
Then every $A \in \ker\pi$ satisfies $\mathrm{rk}(A) \leq d-1$: so $\ker\pi \cap \mathcal{C} = \{0\}$.
In particular $\pi : \mathcal{C} \to \mathbb{F}^{n\times(m-d+1)}$ is injective. □

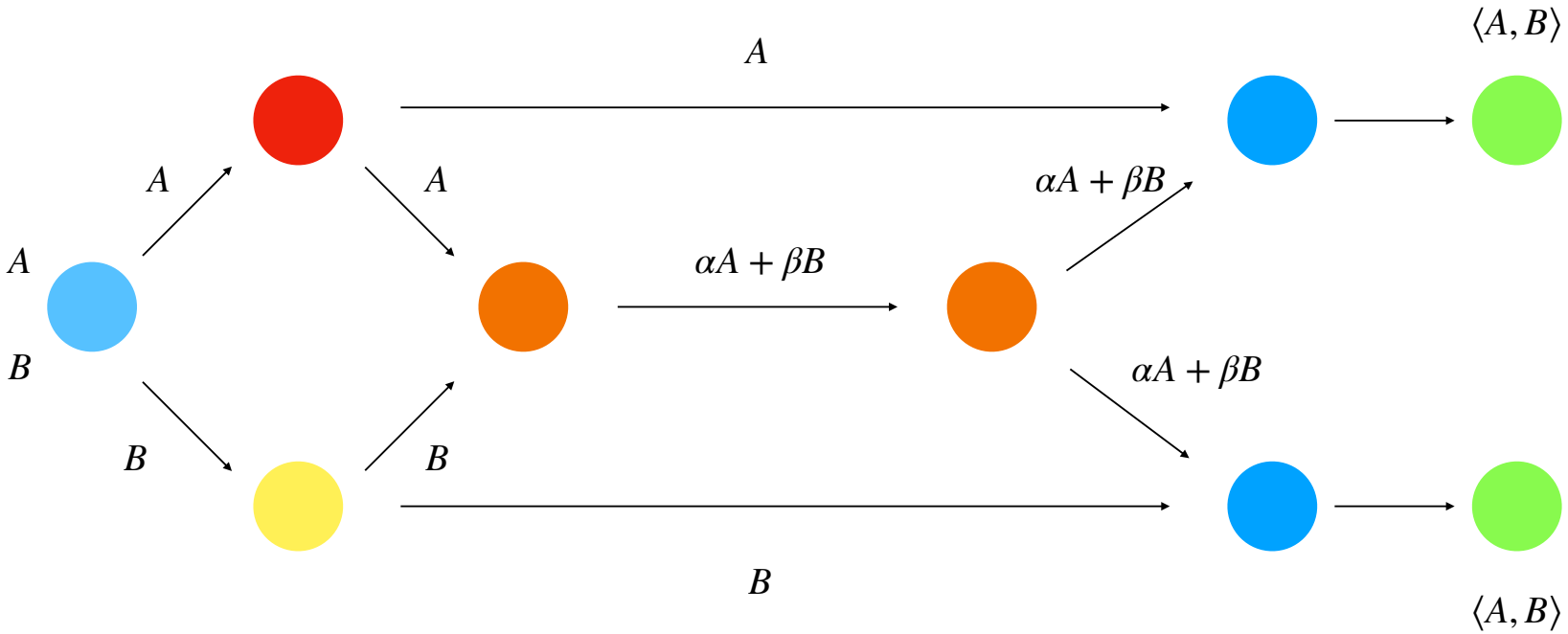
Corollary. If $m = n$, then $k \leq n(n-d+1)$.

Study of rank-metric codes motivated by linear network coding.

Study of rank-metric codes motivated by linear network coding.



Study of rank-metric codes motivated by linear network coding.



The information that gets carried into the Network is a subspace of $\mathbb{F}^n$. So we move to work with the **Grassmannian**

$$\mathrm{Gr}_{\mathbb{F}}(n) = \{U \text{ subspace of } \mathbb{F}^n\}$$

with the **injection distance**:

$$d_I(V, W) = \frac{1}{2}(\dim_{\mathbb{F}}(V + W) - \dim_{\mathbb{F}}(V \cap W)).$$

The information that gets carried into the Network is a subspace of $\mathbb{F}^n$. So we move to work with the **Grassmannian**

$$\mathrm{Gr}_{\mathbb{F}}(n) = \{U \text{ subspace of } \mathbb{F}^n\}$$

with the **injection distance**:

$$d_I(V, W) = \frac{1}{2}(\dim_{\mathbb{F}}(V + W) - \dim_{\mathbb{F}}(V \cap W)).$$

If $V, W \in \mathrm{Gr}_{\mathbb{F}}(m, n) = \{U \text{ subspace of } \mathbb{F}^n, \dim_{\mathbb{F}} U = m\}$, then this rewrites as

$$d_I(V, W) = m - \dim_{\mathbb{F}}(V \cap W).$$

The information that gets carried into the Network is a subspace of $\mathbb{F}^n$. So we move to work with the **Grassmannian**

$$\mathrm{Gr}_{\mathbb{F}}(n) = \{U \text{ subspace of } \mathbb{F}^n\}$$

with the **injection distance**:

$$d_I(V,W) = \frac{1}{2}(\dim_{\mathbb{F}}(V+W) - \dim_{\mathbb{F}}(V \cap W)).$$

If $V, W \in \mathrm{Gr}_{\mathbb{F}}(m,n) = \{U \text{ subspace of } \mathbb{F}^n, \dim_{\mathbb{F}} U = m\}$, then this rewrites as

$$d_I(V,W) = m - \dim_{\mathbb{F}}(V \cap W).$$

Problem. The Grassmannian is not a linear code.

Each Grassmannian $\mathrm{Gr}_{\mathbb{F}}(m,n)$ can be decomposed into Schubert cells, corresponding to the possible pivots in a matrix representation of its elements:

$$\mathrm{Gr}_{\mathbb{F}}^{\{1,2\}}(2,4) = \left\{ \mathrm{rowspan}_{\mathbb{F}} \begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & c & d \end{pmatrix} : a,b,c,d \in \mathbb{F} \right\}$$

$$\mathrm{Gr}_{\mathbb{F}}^{\{1,3\}}(2,4) = \left\{ \mathrm{rowspan}_{\mathbb{F}} \begin{pmatrix} 1 & e & 0 & f \\ 0 & 0 & 1 & g \end{pmatrix} : e,f,g \in \mathbb{F} \right\}$$

Each Grassmannian $\mathrm{Gr}_{\mathbb{F}}(m,n)$ can be decomposed into Schubert cells, corresponding to the possible pivots in a matrix representation of its elements:

$$\mathrm{Gr}_{\mathbb{F}}^{\{1,2\}}(2,4) = \left\{ \mathrm{rowspan}_{\mathbb{F}} \begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & c & d \end{pmatrix} : a,b,c,d \in \mathbb{F} \right\}$$

$$\mathrm{Gr}_{\mathbb{F}}^{\{1,3\}}(2,4) = \left\{ \mathrm{rowspan}_{\mathbb{F}} \begin{pmatrix} 1 & e & 0 & f \\ 0 & 0 & 1 & g \end{pmatrix} : e,f,g \in \mathbb{F} \right\}$$

The largest cell $\mathrm{Gr}_{\mathbb{F}}^{\circ}(m,n)$ corresponds to the pivots $\{1,\ldots,m\}$.

Each Grassmannian $\mathrm{Gr}_{\mathbb{F}}(m,n)$ can be decomposed into Schubert cells, corresponding to the possible pivots in a matrix representation of its elements:

$$\mathrm{Gr}_{\mathbb{F}}^{\{1,2\}}(2,4) = \left\{ \mathrm{rowspan}_{\mathbb{F}} \begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & c & d \end{pmatrix} : a,b,c,d \in \mathbb{F} \right\}$$

$$\mathrm{Gr}_{\mathbb{F}}^{\{1,3\}}(2,4) = \left\{ \mathrm{rowspan}_{\mathbb{F}} \begin{pmatrix} 1 & e & 0 & f \\ 0 & 0 & 1 & g \end{pmatrix} : e,f,g \in \mathbb{F} \right\}$$

The largest cell $\mathrm{Gr}_{\mathbb{F}}^{\circ}(m,n)$ corresponds to the pivots $\{1,\ldots,m\}$.

Theorem (Silva / Kötter, Kschischang, 2008)

$(\mathrm{Gr}_{\mathbb{F}}^{\circ}(m,n), d_I)$ is isometric to $(\mathbb{F}^{m\times(n-m)}, d_{\mathrm{rk}})$.

Each Grassmannian $\mathrm{Gr}_{\mathbb{F}}(m,n)$ can be decomposed into Schubert cells, corresponding to the possible pivots in a matrix representation of its elements:

$$\mathrm{Gr}_{\mathbb{F}}^{\{1,2\}}(2,4) = \left\{ \mathrm{rowspan}_{\mathbb{F}} \begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & c & d \end{pmatrix} : a,b,c,d \in \mathbb{F} \right\}$$

$$\mathrm{Gr}_{\mathbb{F}}^{\{1,3\}}(2,4) = \left\{ \mathrm{rowspan}_{\mathbb{F}} \begin{pmatrix} 1 & e & 0 & f \\ 0 & 0 & 1 & g \end{pmatrix} : e,f,g \in \mathbb{F} \right\}$$

The largest cell $\mathrm{Gr}_{\mathbb{F}}^{\circ}(m,n)$ corresponds to the pivots $\{1,\ldots,m\}$.

Theorem (Silva / Kötter, Kschischang, 2008)

$(\mathrm{Gr}_{\mathbb{F}}^{\circ}(m,n), d_I)$ is isometric to $(\mathbb{F}^{m\times(n-m)}, d_{\mathrm{rk}})$.

Remark. Rank-metric codes had already been studied in the 70's by Delsarte and in the 80's by Gabidulin.

Definition. Rank-metric codes for which the Singleton-like bound is tight

$$k = \min\{n(m-d+1), m(n-d+1)\}$$

are called **maximum rank distance (MRD)**.

Definition. Rank-metric codes for which the Singleton-like bound is tight

$$k = \min\{n(m-d+1), m(n-d+1)\}$$

are called **maximum rank distance (MRD)**.

Example. Assume that $n = m$, so that we seek $k = n(n-d+1)$.

- If $d = 1$, then $k = n^2$ and $\mathcal{C} = \mathbb{F}^{n\times n}$ is an MRD code.

Definition. Rank-metric codes for which the Singleton-like bound is tight

$$k = \min\{n(m-d+1), m(n-d+1)\}$$

are called **maximum rank distance (MRD)**.

Example. Assume that $n = m$, so that we seek $k = n(n-d+1)$.

- If $d = 1$, then $k = n^2$ and $\mathcal{C} = \mathbb{F}^{n\times n}$ is an MRD code.
- If $d = n$, then $k = n$. E.g. if $n = 3$ and $\mathbb{F} = \mathbb{F}_2$, then

$$\mathcal{C} = \left\langle \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \right\rangle_{\mathbb{F}} = \left\{ \begin{pmatrix} a & b & c \\ c & a+c & b \\ b & b+c & a+c \end{pmatrix} : a, b, c \in \mathbb{F} \right\}$$

is a $[3 \times 3, 3, 3]_{\mathbb{F}}$ rank-metric code, i.e. an MRD code.

Definition. Rank-metric codes for which the Singleton-like bound is tight

$$k = \min\{n(m-d+1), m(n-d+1)\}$$

are called **maximum rank distance (MRD)**.

Example. Assume that $n = m$, so that we seek $k = n(n-d+1)$.

- If $d = 1$, then $k = n^2$ and $\mathcal{C} = \mathbb{F}^{n\times n}$ is an MRD code.
- If $d = n$, then $k = n$. E.g. if $n = 3$ and $\mathbb{F} = \mathbb{F}_2$, then

$$\mathcal{C} = \left\langle \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \right\rangle_{\mathbb{F}} = \left\{ \begin{pmatrix} a & b & c \\ c & a+c & b \\ b & b+c & a+c \end{pmatrix} : a, b, c \in \mathbb{F} \right\}$$

is a $[3 \times 3, 3, 3]_{\mathbb{F}}$ rank-metric code, i.e. an MRD code.

Constructing MRD codes has been and still is an important research problem!

A construction of Gabidulin for finite fields (later generalized by Guralnick) goes as follows.

A construction of Gabidulin for finite fields (later generalized by Guralnick) goes as follows.

Assume $\mathbb{F}$ is finite and let $\mathbb{L}$ be a cyclic degree n extension of $\mathbb{F}$, with Galois group $\mathrm{Gal}(\mathbb{L}/\mathbb{F}) = \langle \sigma \rangle$. Endowing

$$\mathbb{L}[\sigma] = \left\{ \sum_{i=0}^{n-1} a_i \sigma^i \ : \ a_i \in \mathbb{L} \right\}$$

A construction of Gabidulin for finite fields (later generalized by Guralnick) goes as follows.

Assume $\mathbb{F}$ is finite and let $\mathbb{L}$ be a cyclic degree n extension of $\mathbb{F}$, with Galois group $\mathrm{Gal}(\mathbb{L}/\mathbb{F}) = \langle \sigma \rangle$. Endowing

$$\mathbb{L}[\sigma] = \left\{ \sum_{i=0}^{n-1} a_i \sigma^i \ : \ a_i \in \mathbb{L} \right\}$$

with the multiplication defined on monomials as

$$(a\sigma^i) \cdot (b\sigma^j) = a\sigma^i(b)\sigma^{i+j}, \qquad \text{for } a, b \in \mathbb{L},$$

A construction of Gabidulin for finite fields (later generalized by Guralnick) goes as follows.

Assume $\mathbb{F}$ is finite and let $\mathbb{L}$ be a cyclic degree n extension of $\mathbb{F}$, with Galois group $\mathrm{Gal}(\mathbb{L}/\mathbb{F}) = \langle\sigma\rangle$. Endowing

$$\mathbb{L}[\sigma] = \left\{ \sum_{i=0}^{n-1} a_i \sigma^i \ : \ a_i \in \mathbb{L} \right\}$$

with the multiplication defined on monomials as

$$(a\sigma^i) \cdot (b\sigma^j) = a\sigma^i(b)\sigma^{i+j}, \qquad \text{for } a, b \in \mathbb{L},$$

we have an $\mathbb{F}$-algebra isomorphism:

$$\mathbb{L}[\sigma] \longrightarrow \mathrm{End}_{\mathbb{F}}(\mathbb{L}), \quad \sum_{i=0}^{n-1} a_i \sigma^i \longmapsto \left(\alpha \longmapsto \sum_{i=0}^{n-1} a_i \sigma^i(\alpha) \right).$$

Fixing a basis of $\mathbb{L}$ over $\mathbb{F}$ induces then an isomorphism

$$\mathrm{M} : \mathbb{L}[\sigma] \longrightarrow \mathrm{End}_{\mathbb{F}}(\mathbb{L}) \longrightarrow \mathbb{F}^{n\times n}.$$

Fixing a basis of $\mathbb{L}$ over $\mathbb{F}$ induces then an isomorphism

$$\mathrm{M} : \mathbb{L}[\sigma] \longrightarrow \mathrm{End}_{\mathbb{F}}(\mathbb{L}) \longrightarrow \mathbb{F}^{n\times n}.$$

Taking $1 \leq d \leq n$, the $\mathbb{L}$-subspace

$$\mathbb{L}[\sigma]_{n-d} = \left\{ \sum_{i=0}^{n-d} a_i \sigma^i \ : \ a_i \in \mathbb{L} \right\} \subseteq \mathbb{L}[\sigma]$$

has $\mathbb{F}$-dimension $n(n-d+1)$ and every $p(\sigma) \in \mathbb{L}[\sigma]_{n-d}$ satisfies:

Fixing a basis of $\mathbb{L}$ over $\mathbb{F}$ induces then an isomorphism

$$\mathrm{M} : \mathbb{L}[\sigma] \longrightarrow \mathrm{End}_{\mathbb{F}}(\mathbb{L}) \longrightarrow \mathbb{F}^{n\times n}.$$

Taking $1 \leq d \leq n$, the $\mathbb{L}$-subspace

$$\mathbb{L}[\sigma]_{n-d} = \left\{ \sum_{i=0}^{n-d} a_i \sigma^i \ : \ a_i \in \mathbb{L} \right\} \subseteq \mathbb{L}[\sigma]$$

has $\mathbb{F}$-dimension $n(n-d+1)$ and every $p(\sigma) \in \mathbb{L}[\sigma]_{n-d}$ satisfies:

$$\begin{aligned} & \dim_{\mathbb{F}}(\ker p(\sigma)) \leq \deg p(\sigma) \leq n-d \\ \rightsquigarrow \quad & \mathrm{rk}\, \mathrm{M}(p(\sigma)) \geq n - (n-d) = d. \end{aligned}$$

Fixing a basis of $\mathbb{L}$ over $\mathbb{F}$ induces then an isomorphism

$$\mathrm{M} : \mathbb{L}[\sigma] \longrightarrow \mathrm{End}_{\mathbb{F}}(\mathbb{L}) \longrightarrow \mathbb{F}^{n\times n}.$$

Taking $1 \leq d \leq n$, the $\mathbb{L}$-subspace

$$\mathbb{L}[\sigma]_{n-d} = \left\{ \sum_{i=0}^{n-d} a_i \sigma^i \ : \ a_i \in \mathbb{L} \right\} \subseteq \mathbb{L}[\sigma]$$

has $\mathbb{F}$-dimension $n(n-d+1)$ and every $p(\sigma) \in \mathbb{L}[\sigma]_{n-d}$ satisfies:

$$\begin{aligned} & \dim_{\mathbb{F}}(\ker p(\sigma)) \leq \deg p(\sigma) \leq n-d \\ \rightsquigarrow \quad & \mathrm{rk}\, \mathrm{M}(p(\sigma)) \geq n - (n-d) = d. \end{aligned}$$

So $\mathrm{M}(\mathbb{L}[\sigma]_{n-d})$ is an $[n \times n, n(n-d+1), d]_{\mathbb{F}}$ rank-metric code: in particular an MRD code!

. . . what if we wanted codes with a prescribed support?
For instance, what if we wanted our matrices to all be upper triangular?

. . . what if we wanted codes with a prescribed support?
For instance, what if we wanted our matrices to all be upper triangular?

Example.

$$\mathrm{Gr}_{\mathbb{F}}^{\{1,2\}}(2,4) = \left\{ \mathrm{rowspan}_{\mathbb{F}} \begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & c & d \end{pmatrix} : a,b,c,d \in \mathbb{F} \right\}$$

$$\mathrm{Gr}_{\mathbb{F}}^{\{1,3\}}(2,4) = \left\{ \mathrm{rowspan}_{\mathbb{F}} \begin{pmatrix} 1 & e & 0 & f \\ 0 & 0 & 1 & g \end{pmatrix} : e,f,g \in \mathbb{F} \right\}$$

. . . what if we wanted codes with a prescribed support? For instance, what if we wanted our matrices to all be upper triangular?

Example.

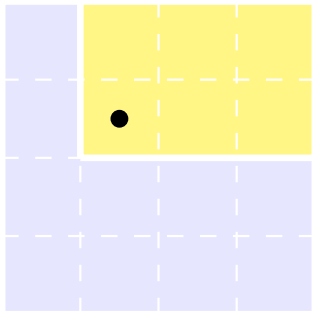
$$\mathrm{Gr}_{\mathbb{F}}^{\{1,2\}}(2,4) = \left\{ \mathrm{rowspan}_{\mathbb{F}} \begin{pmatrix} 1 & 0 & a & b \\ 0 & 1 & c & d \end{pmatrix} : a,b,c,d \in \mathbb{F} \right\}$$

$$\mathrm{Gr}_{\mathbb{F}}^{\{1,3\}}(2,4) = \left\{ \mathrm{rowspan}_{\mathbb{F}} \begin{pmatrix} 1 & e & 0 & f \\ 0 & 0 & 1 & g \end{pmatrix} : e,f,g \in \mathbb{F} \right\}$$

can be identically described by the 2×2 diagrams:

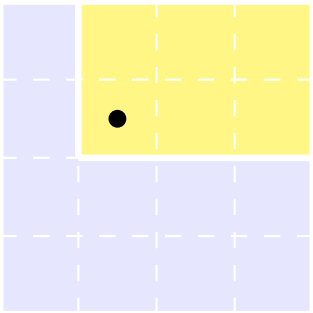
Definition. A **Ferrers diagram of order** n is a subset $\mathcal{D}$ of $[n]^2 = \{1, \ldots, n\}^2$ such that

- $(i, j) \in \mathcal{D}$ and $j' \geq j \Rightarrow (i, j') \in \mathcal{D}$;
- $(i, j) \in \mathcal{D}$ and $i' \leq i \Rightarrow (i', j) \in \mathcal{D}$.



Definition. A **Ferrers diagram of order** n is a subset $\mathcal{D}$ of $[n]^2 = \{1, \ldots, n\}^2$ such that

- $(i, j) \in \mathcal{D}$ and $j' \geq j \Rightarrow (i, j') \in \mathcal{D}$;
- $(i, j) \in \mathcal{D}$ and $i' \leq i \Rightarrow (i', j) \in \mathcal{D}$.



A given Ferrers diagram of orden n can be also represented as:

- a vector $(c_1, \ldots, c_n)$ where $c_i \leq c_{i+1}$; or
- graphically as an $n \times n$ grid with dots corresponding to the elements of $\mathcal{D}$.

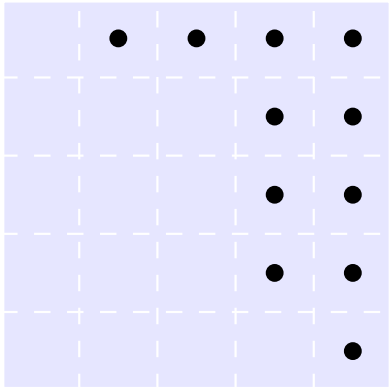
Example. Let $\mathcal{D} \subseteq [5]^2$ be given by

$$\mathcal{D} = \{(1,2),(1,3),(1,4),(1,5),(2,4),(2,5),$$
$$(3,4),(3,5),(4,4),(4,5),(5,5)\}$$

Example. Let $\mathcal{D} \subseteq [5]^2$ be given by

$$\mathcal{D} = \{(1,2),(1,3),(1,4),(1,5),(2,4),(2,5),$$
$$(3,4),(3,5),(4,4),(4,5),(5,5)\}$$

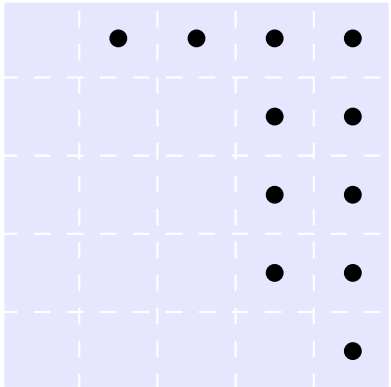
which can be graphically represented as



Example. Let $\mathcal{D} \subseteq [5]^2$ be given by

$$\mathcal{D} = \{(1,2),(1,3),(1,4),(1,5),(2,4),(2,5),$$
$$(3,4),(3,5),(4,4),(4,5),(5,5)\}$$

which can be graphically represented as



or as a vector by $\mathcal{D} = (0,1,1,4,5)$.

Let $\mathcal{D}$ be a Ferrers diagram of order n and define

$$\mathbb{F}^{\mathcal{D}} = \{A \in \mathbb{F}^{n \times n} : (i,j) \in [n]^2 \setminus \mathcal{D} \ \Rightarrow \ a_{ij} = 0\}.$$

Let $\mathcal{D}$ be a Ferrers diagram of order n and define

$$\mathbb{F}^{\mathcal{D}} = \{A \in \mathbb{F}^{n\times n} : (i,j) \in [n]^2 \setminus \mathcal{D} \ \Rightarrow \ a_{ij} = 0\}.$$

Then $\mathcal{D}$ uniquely identifies a set of pivots $P(\mathcal{D})$ of an $n \times 2n$ matrix, so in particular:

Remark.

$(\mathrm{Gr}_{\mathbb{F}}^{P(\mathcal{D})}(n,2n), d_I)$ is isometric to $(\mathbb{F}^{\mathcal{D}}, d_{\mathrm{rk}})$.

Let $\mathcal{D}$ be a Ferrers diagram of order n and define

$$\mathbb{F}^{\mathcal{D}} = \{A \in \mathbb{F}^{n\times n} : (i,j) \in [n]^2 \setminus \mathcal{D} \ \Rightarrow \ a_{ij} = 0\}.$$

Then $\mathcal{D}$ uniquely identifies a set of pivots $P(\mathcal{D})$ of an $n \times 2n$ matrix, so in particular:

Remark.

$$(\mathrm{Gr}_{\mathbb{F}}^{P(\mathcal{D})}(n,2n), d_I) \text{ is isometric to } (\mathbb{F}^{\mathcal{D}}, d_{\mathrm{rk}}).$$

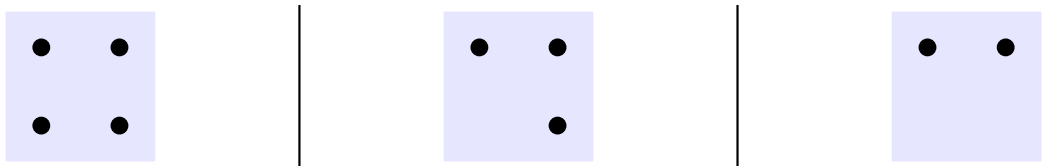
Example. If $\mathcal{D} = [n]^2$, then $\mathbb{F}^{\mathcal{D}} = \mathbb{F}^{n\times n}$ and we recover regular rank-metric codes, i.e. the largest Schubert cell.

Ferrers diagram rank-metric codes $\rangle\, n = 2$

Pivots

$$\begin{pmatrix} 1 & 0 & * & * \\ 0 & 1 & * & * \end{pmatrix} \quad \begin{pmatrix} 1 & * & 0 & * \\ 0 & 0 & 1 & * \end{pmatrix} \quad \begin{pmatrix} 1 & * & * & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

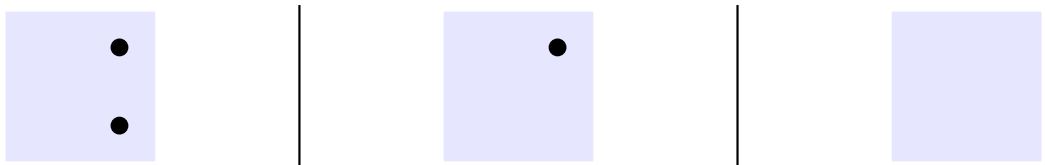
Diagram



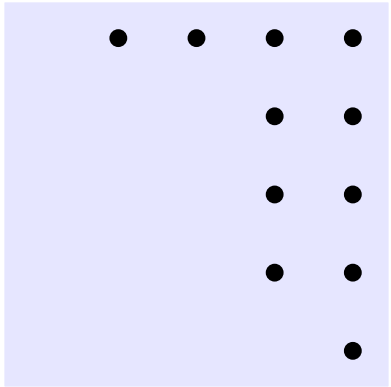
Pivots

$$\begin{pmatrix} 0 & 1 & 0 & * \\ 0 & 0 & 1 & * \end{pmatrix} \quad \begin{pmatrix} 0 & 1 & * & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \begin{pmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

Diagram

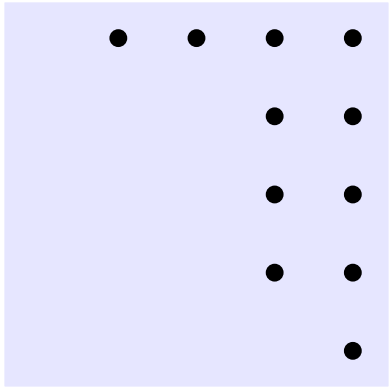


Example. Earlier we looked at

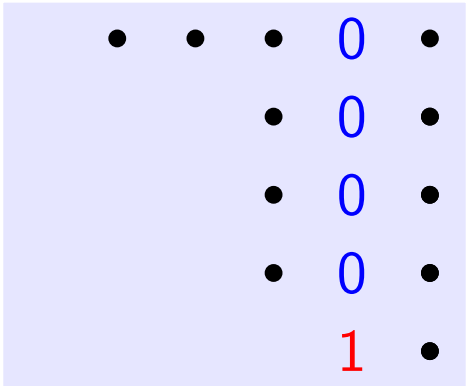


with $n = 5$ and thus $2n = 10$.

Example. Earlier we looked at

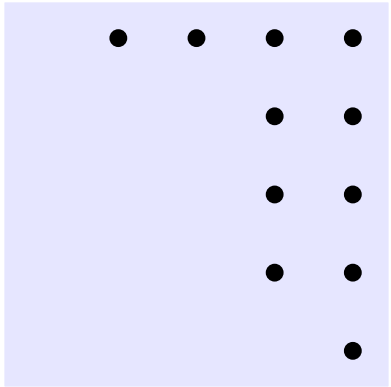


with $n = 5$ and thus $2n = 10$. The corresponding Schubert cell is:

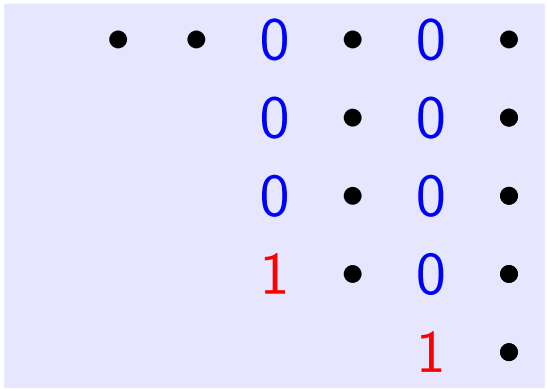


Column count: 6

Example. Earlier we looked at

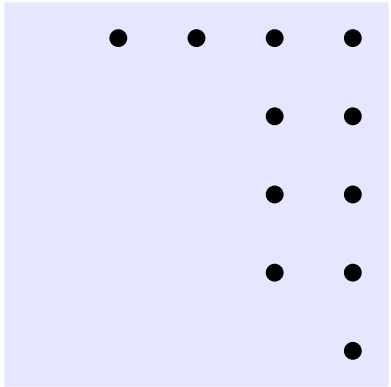


with $n = 5$ and thus $2n = 10$. The corresponding Schubert cell is:

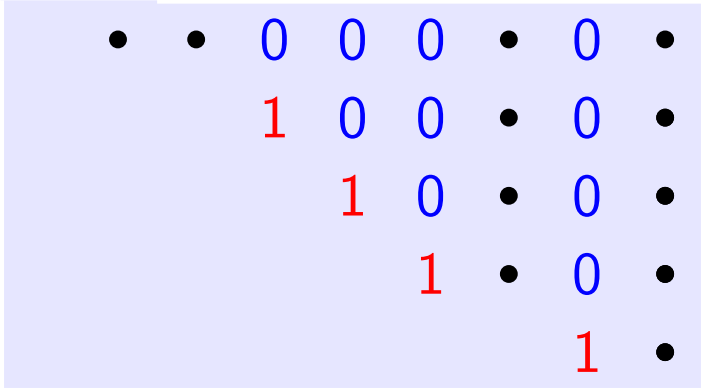


Column count: 7

Example. Earlier we looked at

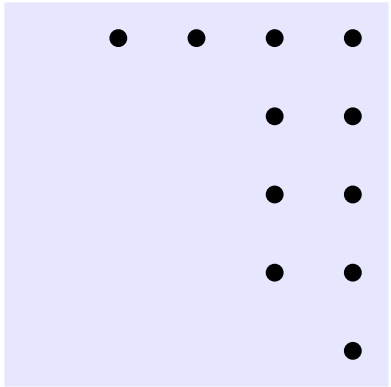


with $n = 5$ and thus $2n = 10$. The corresponding Schubert cell is:

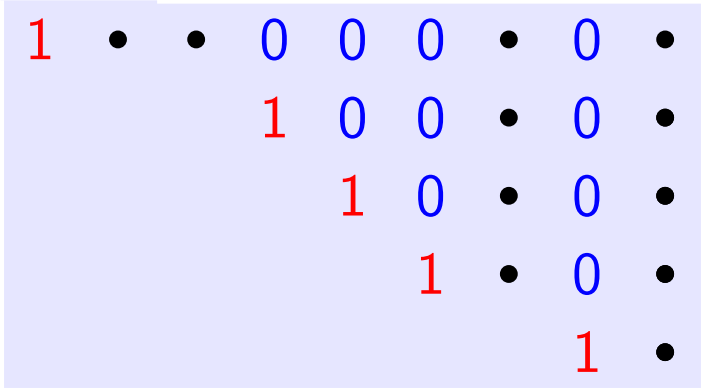


Column count: 9

Example. Earlier we looked at

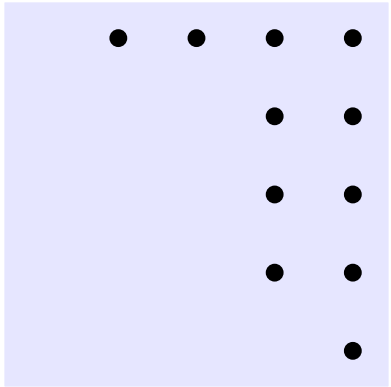


with $n = 5$ and thus $2n = 10$. The corresponding Schubert cell is:

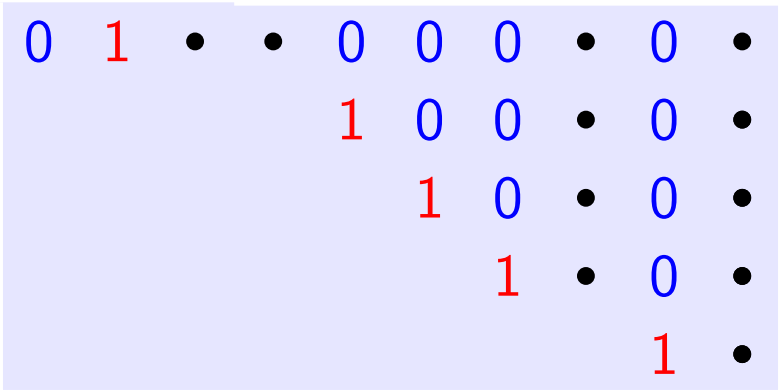


Column count: 9

Example. Earlier we looked at



with $n = 5$ and thus $2n = 10$. The corresponding Schubert cell is:



Column count: 10

Definition. Let $\mathcal{D}$ be a Ferrers diagram of order n. A $[\mathcal{D}, k, d]_{\mathbb{F}}$ **Ferrers diagram rank-metric code** is an $[n \times n, k, d]_{\mathbb{F}}$ rank-metric code $\mathcal{C}$ such that

$$A = (a_{ij}) \in \mathcal{C}, \ a_{k\ell} \neq 0 \implies (k, \ell) \in \mathcal{D}.$$

Equivalently, it is a linear subspace of $\mathbb{F}^{\mathcal{D}}$ of dimension k endowed with the rank metric and with minimum distance equal to d.

Definition. Let $\mathcal{D}$ be a Ferrers diagram of order n. A $[\mathcal{D}, k, d]_{\mathbb{F}}$ **Ferrers diagram rank-metric code** is an $[n \times n, k, d]_{\mathbb{F}}$ rank-metric code $\mathcal{C}$ such that

$$A = (a_{ij}) \in \mathcal{C},\ a_{k\ell} \neq 0 \implies (k, \ell) \in \mathcal{D}.$$

Equivalently, it is a linear subspace of $\mathbb{F}^{\mathcal{D}}$ of dimension k endowed with the rank metric and with minimum distance equal to d.

Example.

- If $\mathcal{D} = [n]^2$, then regular rank-metric codes.
- If $\mathcal{D} = (1, 2, \ldots, n)$, then the $[\mathcal{D}, k, d]_{\mathbb{F}}$ Ferrers diagram rank-metric codes are $[n \times n, k, d]_{\mathbb{F}}$ rank-metric codes contained in the space of upper triangular matrices.

Theorem (Etzion, Silberstein, 2009)

$$k \leq \min_{j=0,\ldots,d-1} \left\{ \sum_{i=1}^{n-j} \max\{0, c_i - d + 1 + j\} \right\} = \nu_{\min}(\mathcal{D}, d).$$

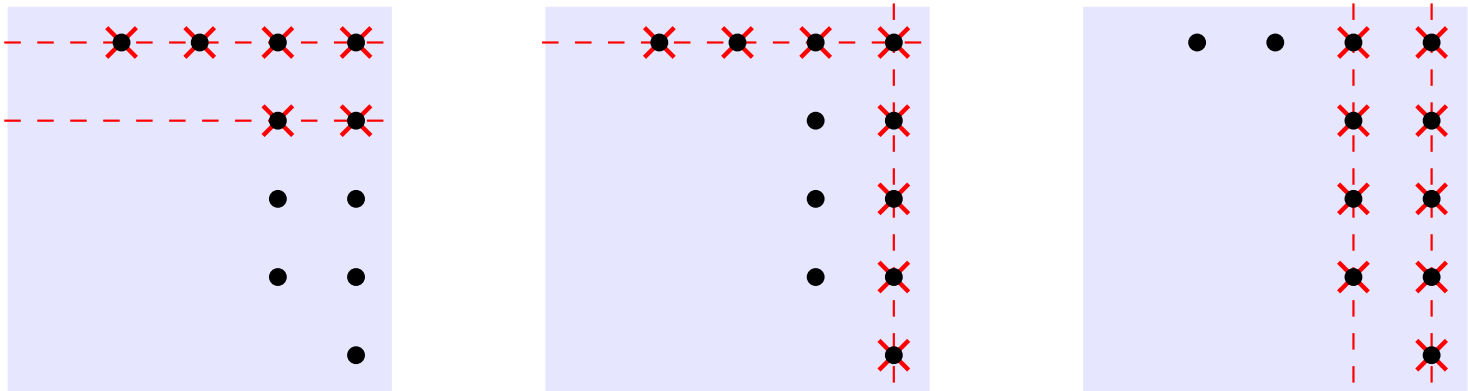
Theorem (Etzion, Silberstein, 2009)

$$k \leq \min_{j=0,\ldots,d-1} \left\{ \sum_{i=1}^{n-j} \max\{0, c_i - d + 1 + j\} \right\} = \nu_{\min}(\mathcal{D}, d).$$

Example. If $\mathcal{D} = (0, 1, 1, 4, 5)$ and $d = 3$, then

$$\nu_{\min}(\mathcal{D}, d) = \min\{2 + 3, 3, 1 + 1\} = 2$$

i.e. it is the minimum number of dots remaining after the deletions:



Conjecture (Etzion, Silberstein, 2009) Let $\mathcal{D}$ be a Ferrers diagram of order n and $d \in \{1, \ldots, n\}$. If $\mathbb{F}$ is a finite field, then there exists a $[\mathcal{D}, k, d]_{\mathbb{F}}$ code $\mathcal{C}$ with $k = \nu_{\min}(\mathcal{D}, d)$.

Conjecture (Etzion, Silberstein, 2009) Let $\mathcal{D}$ be a Ferrers diagram of order n and $d \in \{1, \ldots, n\}$. If $\mathbb{F}$ is a finite field, then there exists a $[\mathcal{D}, k, d]_{\mathbb{F}}$ code $\mathcal{C}$ with $k = \nu_{\min}(\mathcal{D}, d)$.

Definition. A a **maximum Ferrers diagram (MFD) code** is a $[\mathcal{D}, \nu_{\min}(\mathcal{D}, d), d]_{\mathbb{F}}$ Ferrers diagram rank-metric code.

Conjecture (Etzion, Silberstein, 2009) Let $\mathcal{D}$ be a Ferrers diagram of order n and $d \in \{1, \ldots, n\}$. If $\mathbb{F}$ is a finite field, then there exists a $[\mathcal{D}, k, d]_{\mathbb{F}}$ code $\mathcal{C}$ with $k = \nu_{\min}(\mathcal{D}, d)$.

Definition. A a **maximum Ferrers diagram (MFD) code** is a $[\mathcal{D}, \nu_{\min}(\mathcal{D}, d), d]_{\mathbb{F}}$ Ferrers diagram rank-metric code.

Example. Assume $\mathcal{D} = (1, 2, \ldots, n)$. At the beginning of 2022 the existence of MFD codes had been proven for:

- $d = 1$ (easy)
- $d = 2$ (taking subspace with sum zero diagonals)
- $d = 3$ or $d = n - 1$ (Antrobus, Gluesing-Luerssen, 2019)
- $|\mathbb{F}| \geq n - 1$ (MDS-constructible pairs; Etzion, Gorla, Ravagnani, Wachter-Zeh, 2016)

Conjecture (Etzion, Silberstein, 2009) Let $\mathcal{D}$ be a Ferrers diagram of order n and $d \in \{1, \ldots, n\}$. If $\mathbb{F}$ is a finite field, then there exists a $[\mathcal{D}, k, d]_{\mathbb{F}}$ code $\mathcal{C}$ with $k = \nu_{\min}(\mathcal{D}, d)$.

Definition. A a **maximum Ferrers diagram (MFD) code** is a $[\mathcal{D}, \nu_{\min}(\mathcal{D}, d), d]_{\mathbb{F}}$ Ferrers diagram rank-metric code.

Example. Assume $\mathcal{D} = (1, 2, \ldots, n)$. At the beginning of 2022 the existence of MFD codes had been proven for:

- $d = 1$ (easy)
- $d = 2$ (taking subspace with sum zero diagonals)
- $d = 3$ or $d = n - 1$ (Antrobus, Gluesing-Luerssen, 2019)
- $|\mathbb{F}| \geq n - 1$ (MDS-constructible pairs; Etzion, Gorla, Ravagnani, Wachter-Zeh, 2016)

WE STARTED FROM HERE!

Upper triangular matrices can be interpreted as the stabilizer in $\mathbb{F}^{n\times n}$ of the maximal $\mathbb{F}$-flag

$$\mathcal{F}: \quad \mathcal{F}_0 = 0 < \mathcal{F}_1 = \mathbb{F}e_1 < \mathcal{F}_2 = \mathbb{F}e_1 \oplus \mathbb{F}e_2 < \ldots < \mathcal{F}_n = \mathbb{F}^n$$

given by the standard basis.

Upper triangular matrices can be interpreted as the stabilizer in $\mathbb{F}^{n\times n}$ of the maximal $\mathbb{F}$-flag

$$\mathcal{F}: \quad \mathcal{F}_0 = 0 < \mathcal{F}_1 = \mathbb{F}e_1 < \mathcal{F}_2 = \mathbb{F}e_1 \oplus \mathbb{F}e_2 < \ldots < \mathcal{F}_n = \mathbb{F}^n$$

given by the standard basis.

Idea! Rely on Gabidulin's construction and look for:

- a field extension $\mathbb{F} \subset \mathbb{L}$ of degree n with $\mathrm{Gal}(\mathbb{L}/\mathbb{F}) = \langle \sigma \rangle$,

Upper triangular matrices can be interpreted as the stabilizer in $\mathbb{F}^{n\times n}$ of the maximal $\mathbb{F}$-flag

$$\mathcal{F}: \quad \mathcal{F}_0 = 0 < \mathcal{F}_1 = \mathbb{F}e_1 < \mathcal{F}_2 = \mathbb{F}e_1 \oplus \mathbb{F}e_2 < \ldots < \mathcal{F}_n = \mathbb{F}^n$$

given by the standard basis.

Idea! Rely on Gabidulin's construction and look for:

- a field extension $\mathbb{F} \subset \mathbb{L}$ of degree n with $\mathrm{Gal}(\mathbb{L}/\mathbb{F}) = \langle \sigma \rangle$,
- a maximal $\mathbb{F}$-flag in $\mathbb{L}$ together with

Upper triangular matrices can be interpreted as the stabilizer in $\mathbb{F}^{n\times n}$ of the maximal $\mathbb{F}$-flag

$$\mathcal{F}: \quad \mathcal{F}_0 = 0 < \mathcal{F}_1 = \mathbb{F}e_1 < \mathcal{F}_2 = \mathbb{F}e_1 \oplus \mathbb{F}e_2 < \ldots < \mathcal{F}_n = \mathbb{F}^n$$

given by the standard basis.

Idea! Rely on Gabidulin's construction and look for:

- a field extension $\mathbb{F} \subset \mathbb{L}$ of degree n with $\mathrm{Gal}(\mathbb{L}/\mathbb{F}) = \langle\sigma\rangle$,
- a maximal $\mathbb{F}$-flag in $\mathbb{L}$ together with
- a subspace $\mathbb{L}[\sigma;\mathcal{D}]_{n-d}$ of $\mathbb{L}[\sigma]_{n-d}$ of dimension $\nu_{\min}(\mathcal{D},d)$ st.

$$p(\sigma) \in \mathbb{L}[\sigma;\mathcal{D}]_{n-d} \implies p(\mathcal{F}_i) \subseteq \mathcal{F}_i.$$

Upper triangular matrices can be interpreted as the stabilizer in $\mathbb{F}^{n\times n}$ of the maximal $\mathbb{F}$-flag

$$\mathcal{F}: \quad \mathcal{F}_0 = 0 < \mathcal{F}_1 = \mathbb{F}e_1 < \mathcal{F}_2 = \mathbb{F}e_1 \oplus \mathbb{F}e_2 < \ldots < \mathcal{F}_n = \mathbb{F}^n$$

given by the standard basis.

Idea! Rely on Gabidulin's construction and look for:

- a field extension $\mathbb{F} \subset \mathbb{L}$ of degree n with $\mathrm{Gal}(\mathbb{L}/\mathbb{F}) = \langle\sigma\rangle$,
- a maximal $\mathbb{F}$-flag in $\mathbb{L}$ together with
- a subspace $\mathbb{L}[\sigma;\mathcal{D}]_{n-d}$ of $\mathbb{L}[\sigma]_{n-d}$ of dimension $\nu_{\min}(\mathcal{D},d)$ st.

$$p(\sigma) \in \mathbb{L}[\sigma;\mathcal{D}]_{n-d} \implies p(\mathcal{F}_i) \subseteq \mathcal{F}_i.$$

Tricky! Finding the right basis to work with.

Write $p = \mathrm{char}(\mathbb{F})$ and assume $n = p^m$. Then:

- Let $\mathbb{F} \subset \mathbb{L}$ be cyclic of degree n and $\mathrm{Gal}(\mathbb{L}/\mathbb{F}) = \langle \sigma \rangle$.

Write $p = \mathrm{char}(\mathbb{F})$ and assume $n = p^m$. Then:

- Let $\mathbb{F} \subset \mathbb{L}$ be cyclic of degree n and $\mathrm{Gal}(\mathbb{L}/\mathbb{F}) = \langle \sigma \rangle$.
- Define $\overline{\sigma} = \sigma - 1 \in \mathbb{L}[\sigma]$.

Write $p = \mathrm{char}(\mathbb{F})$ and assume $n = p^m$. Then:

- Let $\mathbb{F} \subset \mathbb{L}$ be cyclic of degree n and $\mathrm{Gal}(\mathbb{L}/\mathbb{F}) = \langle \sigma \rangle$.
- Define $\overline{\sigma} = \sigma - 1 \in \mathbb{L}[\sigma]$.
- For each $i \in \{0, \ldots, n\}$, let $\mathcal{F}_i = \ker \overline{\sigma}^i$.

Then $\mathcal{B} = \{\overline{\sigma}^i : i = 0, \ldots, n-1\}$ is an $\mathbb{L}$-basis of $\mathbb{L}[\sigma]$ and

$$\mathcal{F}_0 = 0 < \mathcal{F}_1 = \mathbb{F} < \mathcal{F}_2 < \ldots < \mathcal{F}_n = \mathbb{L}$$

is a maximal $\mathbb{F}$-flag of $\mathbb{L}$.

Write $p = \mathrm{char}(\mathbb{F})$ and assume $n = p^m$. Then:

- Let $\mathbb{F} \subset \mathbb{L}$ be cyclic of degree n and $\mathrm{Gal}(\mathbb{L}/\mathbb{F}) = \langle \sigma \rangle$.
- Define $\overline{\sigma} = \sigma - 1 \in \mathbb{L}[\sigma]$.
- For each $i \in \{0, \ldots, n\}$, let $\mathcal{F}_i = \ker \overline{\sigma}^i$.

Then $\mathcal{B} = \{\overline{\sigma}^i : i = 0, \ldots, n-1\}$ is an $\mathbb{L}$-basis of $\mathbb{L}[\sigma]$ and

$$\mathcal{F}_0 = 0 < \mathcal{F}_1 = \mathbb{F} < \mathcal{F}_2 < \ldots < \mathcal{F}_n = \mathbb{L}$$

is a maximal $\mathbb{F}$-flag of $\mathbb{L}$.

Theorem (Neri, S., 2023+) Let $\mathcal{D} = (1, \ldots, n)$. Then the restriction of $\mathbb{L}[\sigma] \to \mathbb{F}^{n \times n}$ induces an isomorphism

$$\mathbb{L}[\mathcal{D}; \sigma] = \bigoplus_{i=1}^{n} \mathcal{F}_i \overline{\sigma}^i \longrightarrow \mathbb{F}^{\mathcal{D}}.$$

Write $p = \mathrm{char}(\mathbb{F})$ and assume $n = p^m$.

Theorem (Neri, S., 2023+) Let $\mathcal{D} = (1, \ldots, n)$. Then

$$\begin{aligned}\mathbb{L}[\mathcal{D}; \sigma]_{n-d} &= \mathbb{L}[\sigma]_{n-d} \cap \mathbb{L}[\mathcal{D}; \sigma] \\ &= \{p(\sigma) \in \mathbb{L}[\mathcal{D}; \sigma] : \deg p(\sigma) \leq n - d\}\end{aligned}$$

is a $[\mathcal{D}, \nu_{\min}(\mathcal{D}, d), d]_{\mathbb{F}}$ Ferrers diagram rank-metric code.

Write $p = \mathrm{char}(\mathbb{F})$ and assume $n = p^m$.

Theorem (Neri, S., 2023+) Let $\mathcal{D} = (1, \ldots, n)$. Then

$$\begin{aligned}\mathbb{L}[\mathcal{D}; \sigma]_{n-d} &= \mathbb{L}[\sigma]_{n-d} \cap \mathbb{L}[\mathcal{D}; \sigma] \\ &= \{p(\sigma) \in \mathbb{L}[\mathcal{D}; \sigma] : \deg p(\sigma) \leq n - d\}\end{aligned}$$

is a $[\mathcal{D}, \nu_{\min}(\mathcal{D}, d), d]_{\mathbb{F}}$ Ferrers diagram rank-metric code.

Remark. This theorem holds with the more general assumption that $\mathcal{D} = (c_1, \ldots, c_n)$ is **(p-)monotone**:

$$0 < c_i < n \Longrightarrow c_{i+1} > c_i.$$

Write $p = \mathrm{char}(\mathbb{F})$ and assume $n = p^m$.

Theorem (Neri, S., 2023+) Let $\mathcal{D} = (1, \ldots, n)$. Then

$$\begin{aligned}\mathbb{L}[\mathcal{D}; \sigma]_{n-d} &= \mathbb{L}[\sigma]_{n-d} \cap \mathbb{L}[\mathcal{D}; \sigma] \\ &= \{p(\sigma) \in \mathbb{L}[\mathcal{D}; \sigma] : \deg p(\sigma) \leq n - d\}\end{aligned}$$

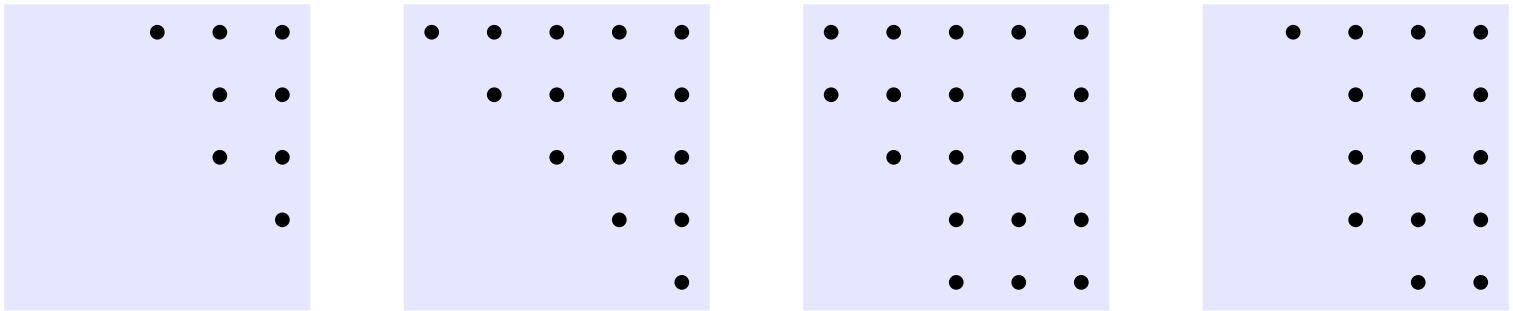
is a $[\mathcal{D}, \nu_{\min}(\mathcal{D}, d), d]_{\mathbb{F}}$ Ferrers diagram rank-metric code.

Remark. This theorem holds with the more general assumption that $\mathcal{D} = (c_1, \ldots, c_n)$ is **(p-)monotone**:

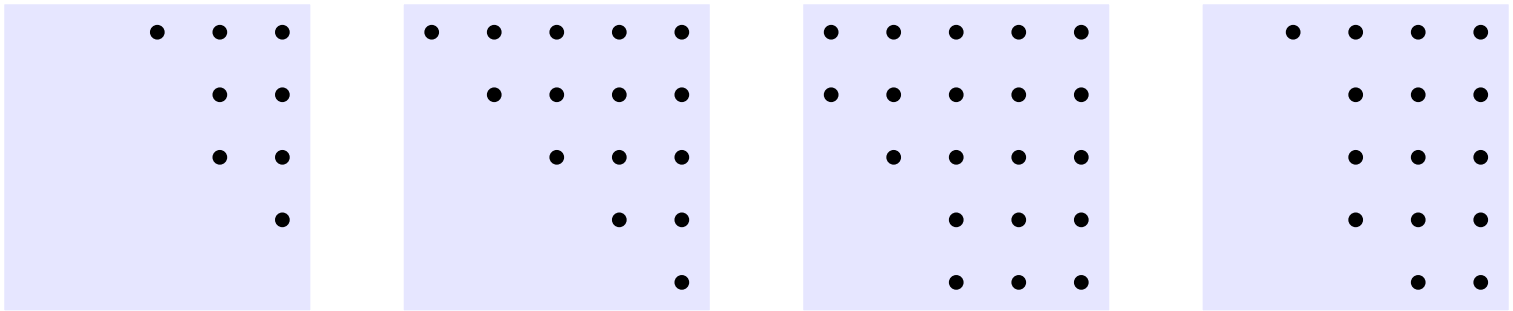
$$0 < c_i < n \Longrightarrow c_{i+1} > c_i.$$

In this case take: $\mathbb{L}[\mathcal{D}; \sigma] = \bigoplus_{i=1}^{n} \mathcal{F}_{c_i} \overline{\sigma}^i$.

$\mathcal{D} = (0, 0, 1, 3, 4)$, $\mathcal{D} = (1, 2, 3, 4, 5)$, $\mathcal{D} = (2, 3, 5, 5, 5)$, $\mathcal{D} = (0, 1, 4, 5, 5)$



$\mathcal{D} = (0, 0, 1, 3, 4)$, $\mathcal{D} = (1, 2, 3, 4, 5)$, $\mathcal{D} = (2, 3, 5, 5, 5)$, $\mathcal{D} = (0, 1, 4, 5, 5)$

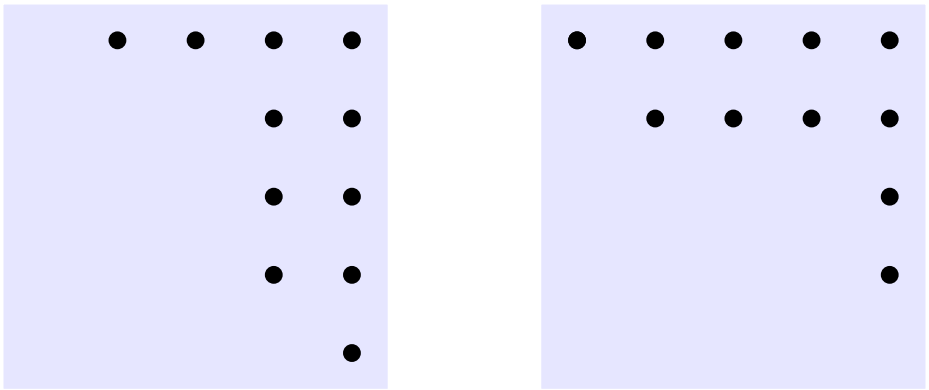


The first two Ferrers diagrams are **(p-)strictly monotone**:

$$0 < c_i \Longrightarrow c_{i+1} > c_i.$$

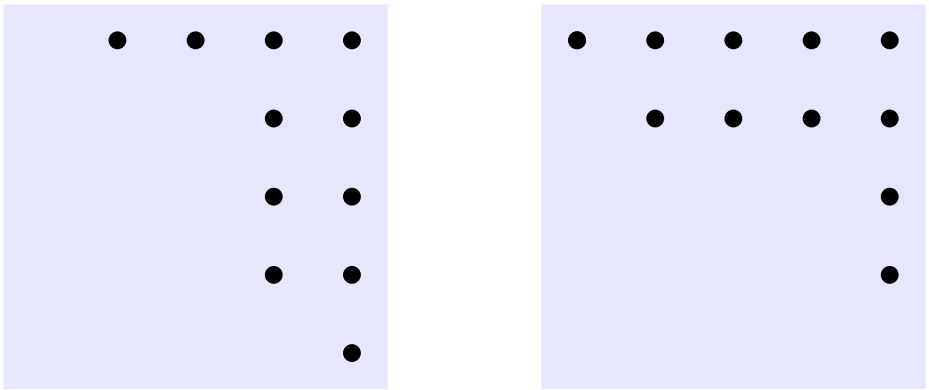
Remark. If the Etzion-Silberstein conjecture holds for $(\mathcal{D}, d)$, then it also holds for $(\mathcal{D}^\top, d)$ where

$$\mathcal{D}^\top = \{(n+1-j, n+1-i) : (i,j) \in \mathcal{D}\}$$



Remark. If the Etzion-Silberstein conjecture holds for $(\mathcal{D}, d)$, then it also holds for $(\mathcal{D}^\top, d)$ where

$$\mathcal{D}^\top = \{(n+1-j, n+1-i) : (i,j) \in \mathcal{D}\}$$



Theorem (Neri, S., 2023+) Let $\mathbb{F}$ be a finite field of characteristic p and let $n = p^m$. Let $\mathcal{D}$ be a Ferrers diagram of order n such that $\mathcal{D}$ or $\mathcal{D}^\top$ is p-monotone and let $1 \leq d \leq n$. Then the Etzion-Silberstein conjecture holds for $(\mathcal{D}, d)$.

Remark. If $\mathcal{D} = (c_1, \ldots, c_n)$ is strictly monotone, then $\mathcal{D}' = (0, c_1, \ldots, c_n)$ is strictly monotone.

Remark. If $\mathcal{D} = (c_1, \ldots, c_n)$ is strictly monotone, then $\mathcal{D}' = (0, c_1, \ldots, c_n)$ is strictly monotone.

Idea! Embed $\mathbb{F}^{\mathcal{D}}$ into a larger $\mathbb{F}^{\mathcal{D}'}$ with $\mathcal{D}'$ of order $n' = p^m$.

Remark. If $\mathcal{D} = (c_1, \ldots, c_n)$ is strictly monotone, then $\mathcal{D}' = (0, c_1, \ldots, c_n)$ is strictly monotone.

Idea! Embed $\mathbb{F}^{\mathcal{D}}$ into a larger $\mathbb{F}^{\mathcal{D}'}$ with $\mathcal{D}'$ of order $n' = p^m$.

Theorem (Neri, S., 2023+) Let $\mathbb{F}$ be a finite field and let $1 \leq d \leq n$ be integers. Let $\mathcal{D}$ be a Ferrers diagram of order n such that $\mathcal{D}$ or $\mathcal{D}^\top$ is strictly monotone. Then the Etzion-Silberstein conjecture holds for $(\mathcal{D}, d)$.

Recall. If $\mathcal{D} = (1, 2, \ldots, n)$, then the conjecture was proven for:

- $d = 1$ (easy)
- $d = 2$ (taking subspace with sum zero diagonals)
- $d = 3$ or $d = n - 1$ (Antrobus, Gluesing-Luerssen, 2019)
- $|\mathbb{F}| \geq n - 1$ (MDS-constructible pairs; Etzion, Gorla, Ravagnani, Wachter-Zeh, 2016)

Recall. If $\mathcal{D} = (1, 2, \ldots, n)$, then the conjecture was proven for:

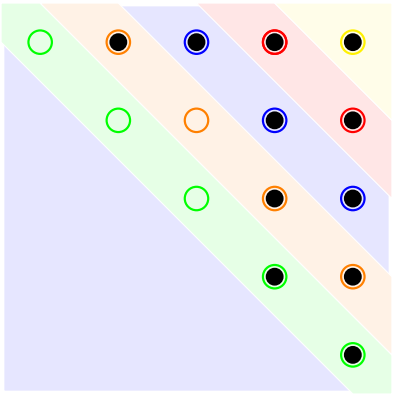
- $d = 1$ (easy)
- $d = 2$ (taking subspace with sum zero diagonals)
- $d = 3$ or $d = n - 1$ (Antrobus, Gluesing-Luerssen, 2019)
- $|\mathbb{F}| \geq n - 1$ (MDS-constructible pairs; Etzion, Gorla, Ravagnani, Wachter-Zeh, 2016)

Definition. The pair $(\mathcal{D}, d)$ is **MDS-constructible** if

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

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

In this case $n = 5$ and, as before, take $d = 3$.

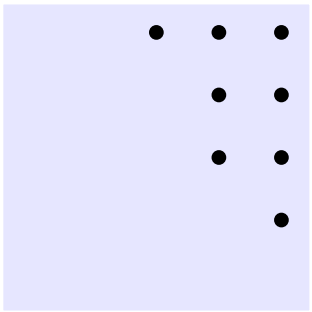


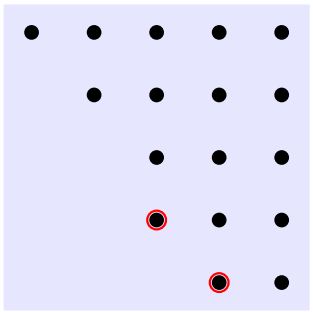
Recall that $\nu_{\min}(\mathcal{D}, 3) = 2$, while

$$\begin{aligned}\nu_{\mathrm{MDS}}(\mathcal{D}, 3) &= \sum_{i=1}^{5} \max\{0, |\mathcal{D} \cap \Delta_i^5| - 3 + 1\} \\ &= 0 + 1 + 1 + 0 + 0 = 2\end{aligned}$$

so $(\mathcal{D}, 3)$ is MDS constructible.

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





d	$\nu_{\min}(\mathcal{D}_1, d)$	$\nu_{\mathrm{MDS}}(\mathcal{D}_1, d)$	$\nu_{\min}(\mathcal{D}_2, d)$	$\nu_{\mathrm{MDS}}(\mathcal{D}_2, d)$
2	4	4	**12**	**10**
3	1	1	**7**	**6**
4	0	0	3	3
5	0	0	1	1

Theorem (Neri, S., 2023+) Let $\mathbb{F}$ be a finite field and let $1 \leq d \leq n$ be integers. Let $\mathcal{D}$ be a Ferrers diagram of order n such that $(\mathcal{D}, d)$ is an MDS pair. Then the Etzion-Silberstein conjecture holds for $(\mathcal{D}, d)$.

Theorem (Neri, S., 2023+) Let $\mathbb{F}$ be a finite field and let $1 \leq d \leq n$ be integers. Let $\mathcal{D}$ be a Ferrers diagram of order n such that $(\mathcal{D}, d)$ is an MDS pair. Then the Etzion-Silberstein conjecture holds for $(\mathcal{D}, d)$.

Remark.

- The proof relies on the conjecture holding true for upper triangular matrices.
- Our result does not ask for additional constraints on the field size!

Check out our preprint on arXiv: 2306.16407