Rank-metric intersecting codes

Martino Borello

(joint work with M. Scotti)

WCC 2026 - 09.06.2026

UNIVERSITÉ PARIS 8 DES CRÉATIONS

Hamming-metric intersecting codes

Definition

$\mathcal{C} \subseteq \mathbb{F}_q^n$ is **intersecting** if $\forall c, c' \in \mathcal{C} \setminus \{0\}$, $\exists i \in \{1, \ldots, n\}$ such that $c_i \cdot c_i' \neq 0$.

Example

$$\mathcal{C} = \left\{ \begin{array}{c} (0,0,0) \\ (1,0,1) \\ (0,1,1) \\ (1,1,0) \end{array} \right\} \subseteq \mathbb{F}_2^3.$$

Why do we care?

Remark

Intersecting codes have **applications** in the following areas:

- **(2, 1)-separating systems** [Friedman, Graham, Ullman, 1969].
- **Communication** over an *AND* channel [Cohen, Lempel, 1985].
- Application to **hash functions** [Körner, Simonyi, 1988].
- **Secret sharing scheme** [Massey, 1993].
- Frameproof codes for **digital fingerprint** [Boneh, Shaw, 1995].
- **Oblivious transfer protocols** [Brassard, Crepeau, Santha, 1996].
- **Genetics problems** [Sagalovich, Chilingarjan, 2009].
- Information on the 2-wise **Davenport constants** [Plagne, Schmid, 2011].
- Information on the generalized 2-wise Davenport constants [B., Schmid, Scotti, 2025] and hence on **factorization in Dedekind domains**.
- **Signature scheme** [Briaud, Gaborit, Neveu, Zémor, 2026].

Rank-metric intersecting codes

Definition

$\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ is **row-intersecting** if $\forall A, B \in \mathcal{C} \setminus \{0\}$,

$$\mathrm{rowsp}(A) \cap \mathrm{rowsp}(B) \neq \{0\}.$$

Example

$$\mathcal{C} = \left\{ \begin{matrix} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \end{matrix} \right\} \subseteq \mathbb{F}_2^{2\times 3}.$$

$\mathbb{F}_{q^m}$-linear case: [Bartoli, B., Marino, Scotti, 2025], [Conca, Jany, Ravagnani, 2026], and...

Rank-metric intersecting codes

Definition

$\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ is **row-intersecting** if $\forall A, B \in \mathcal{C} \setminus \{0\}$,

$$\mathrm{rowsp}(A) \cap \mathrm{rowsp}(B) \neq \{0\}.$$

Example

$$\mathcal{C} = \left\{ \begin{matrix} \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} & \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix} \\ \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} & \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \end{pmatrix} \end{matrix} \right\} \subseteq \mathbb{F}_2^{2\times 3}.$$

$\mathbb{F}_{q^m}$-linear case: [Bartoli, B., Marino, Scotti, 2025], [Conca, Jany, Ravagnani, 2026], and...

see next talk!

Hamming-metric case

Structural properties

Bounds on parameters

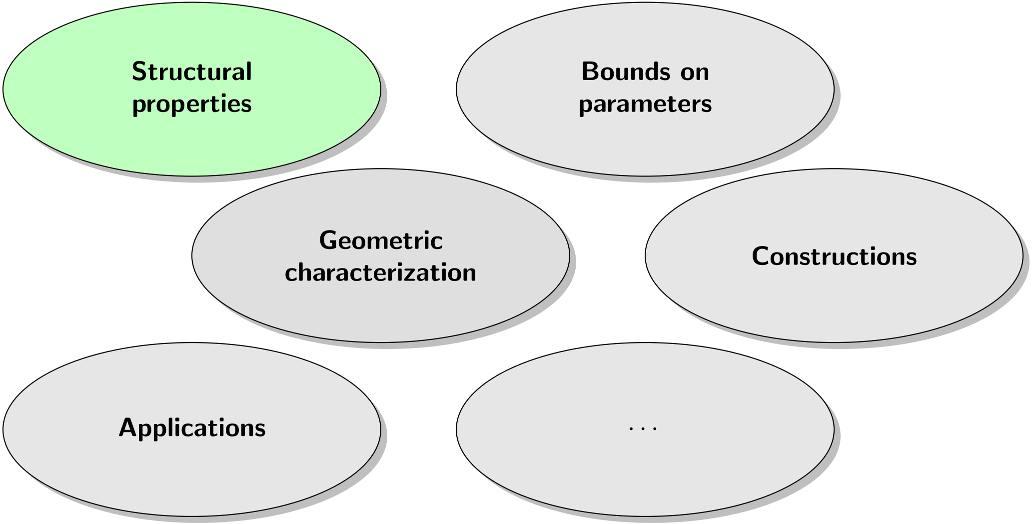
Geometric characterization

Constructions

Applications

...

Rank-metric case



Structural properties

Theorem

Let $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$. $\min_{A\in\mathcal{C}\setminus\{0\}} \mathrm{rk}(A) > \frac{n}{2} \implies \mathcal{C}$ is row-intersecting.

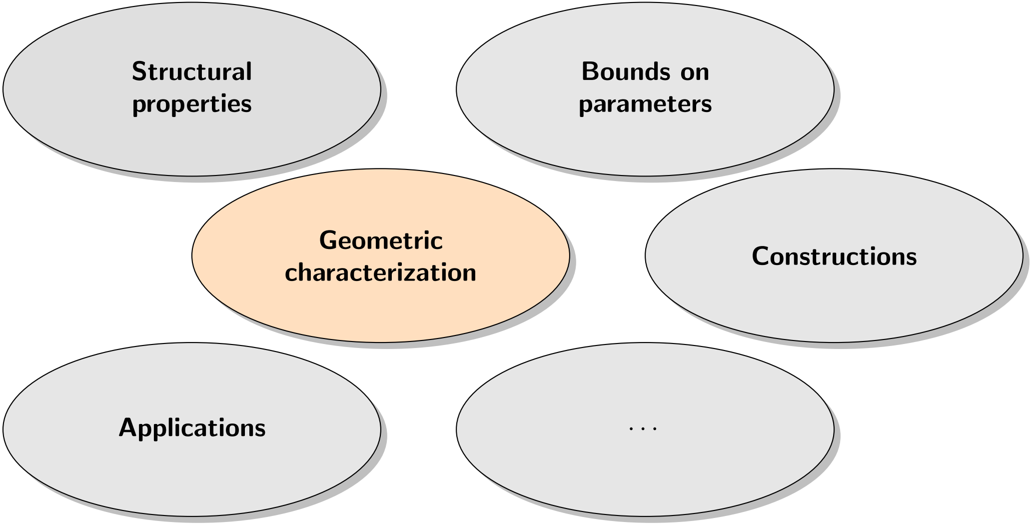
Definition

$\mathcal{C} \in \mathbb{F}_q^{m\times n}$ is **Hamming column-intersecting** (H.c.i.) if $\forall A, B \in \mathcal{C} \setminus \{0\}$, $\exists j$ s.t. the j-th columns of A and B are both nonzero.

Theorem

$\mathcal{C} \in \mathbb{F}_q^{m\times n}$ is row-intersecting $\iff$ $\forall N \in \mathrm{GL}_n(\mathbb{F}_q)$, $\mathcal{C}N := \{AN : A \in \mathcal{C}\}$ is H.c.i..

Rank-metric case



Geometric characterization (Hamming case) [B., Schmid, Scotti, 2025]

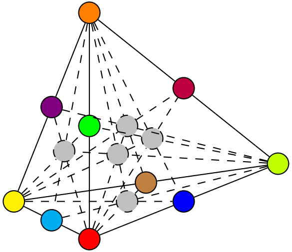
Codes in the Hamming metric corresponds to projective systems.

$\mathcal{C} = \mathrm{rowsp}(G) \subseteq \mathbb{F}_2^{10}$ where

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$\longleftrightarrow$

Projective system in $\mathrm{PG}(3,2)$.



Theorem

$\mathcal{C}$ intersecting $\Leftrightarrow$ the projective system is not contained in the union of two hyperplanes.

Geometric characterization (Hamming case) [B., Schmid, Scotti, 2025]

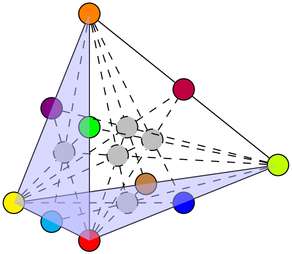
Codes in the Hamming metric corresponds to projective systems.

$\mathcal{C} = \mathrm{rowsp}(G) \subseteq \mathbb{F}_2^{10}$ where

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$\longleftrightarrow$

Projective system in $\mathrm{PG}(3,2)$.



Theorem

$\mathcal{C}$ intersecting $\Leftrightarrow$ the projective system is not contained in the union of two hyperplanes.

Geometric characterization (Hamming case) [B., Schmid, Scotti, 2025]

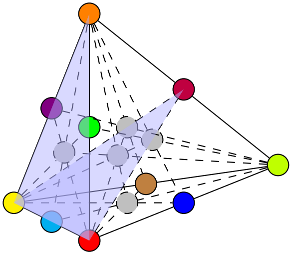
Codes in the Hamming metric corresponds to projective systems.

$\mathcal{C} = \mathrm{rowsp}(G) \subseteq \mathbb{F}_2^{10}$ where

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$\longleftrightarrow$

Projective system in $\mathrm{PG}(3, 2)$.



Theorem

$\mathcal{C}$ intersecting $\Leftrightarrow$ the projective system is not contained in the union of two hyperplanes.

Geometric characterization (Hamming case) [B., Schmid, Scotti, 2025]

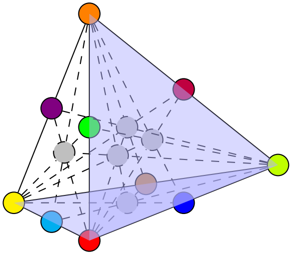
Codes in the Hamming metric corresponds to projective systems.

$\mathcal{C} = \mathrm{rowsp}(G) \subseteq \mathbb{F}_2^{10}$ where

$$G = \begin{bmatrix} 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \end{bmatrix}$$

$\longleftrightarrow$

Projective system in $\mathrm{PG}(3, 2)$.



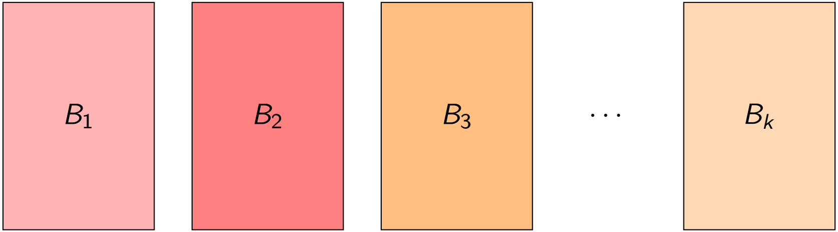
Theorem

$\mathcal{C}$ intersecting $\Leftrightarrow$ the projective system is not contained in the union of two hyperplanes.

Geometric characterization

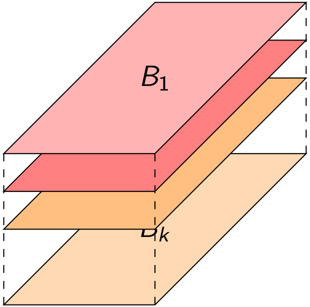
Definition

A (matrix) rank-metric code $\mathcal{C}$ of dimension k in $\mathbb{F}_q^{m\times n}$ can be regarded as the space generated by a 3-tensor $T \in \mathbb{F}_q^k \otimes \mathbb{F}_q^m \otimes \mathbb{F}_q^n \cong \mathbb{F}_q^{k\times m\times n}$ (**Generator tensor**).



Definition

A (matrix) rank-metric code $\mathcal{C}$ of dimension k in $\mathbb{F}_q^{m\times n}$ can be regarded as the space generated by a 3-tensor $T \in \mathbb{F}_q^k \otimes \mathbb{F}_q^m \otimes \mathbb{F}_q^n \cong \mathbb{F}_q^{k\times m\times n}$ (**Generator tensor**).

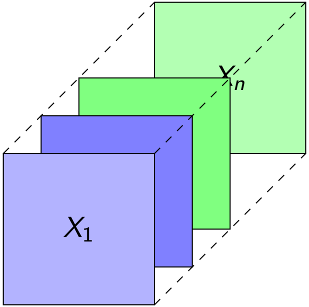


$\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ **(1st slice space)**

Geometric characterization

Definition

A (matrix) rank-metric code $\mathcal{C}$ of dimension k in $\mathbb{F}_q^{m\times n}$ can be regarded as the space generated by a 3-tensor $T \in \mathbb{F}_q^k \otimes \mathbb{F}_q^m \otimes \mathbb{F}_q^n \cong \mathbb{F}_q^{k\times m\times n}$ (**Generator tensor**).



$\mathcal{X} \subseteq \mathbb{F}_q^{k\times m}$ **(3rd slice space)**

[Alfarano, B., Neri, 2026]

Geometric characterization

For $U \subseteq \mathbb{F}_q^k$, $\mathcal{X}(U) := \{X \in \mathcal{X} \,:\, \mathrm{colsp}(X) \subseteq U\}$

Definition

$\mathcal{X} \subseteq \mathbb{F}_q^{k\times m}$ is **column-hyperplane-decomposable** if $\exists H_1, H_2$ hyperplane of $\mathbb{F}_q^k$ s.t.

$$\mathcal{X} = \mathcal{X}(H_1) + \mathcal{X}(H_2).$$

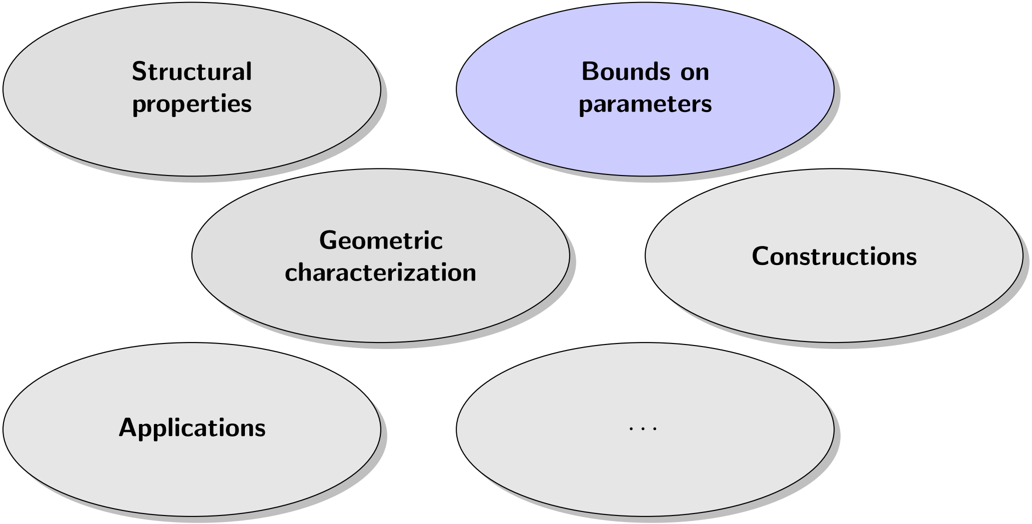
Not hyperplane-decomposable = **column-hyperplane-indecomposable**.

Theorem

$\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ with generator tensor T and $\mathcal{X} \subseteq \mathbb{F}_q^{k\times m}$ the third slice space of T.

$$\mathcal{C} \text{ is row-intersecting} \iff \mathcal{X} \text{ is column-hyperplane-indecomposable.}$$

Rank-metric case



Bounds on parameters

Theorem

If $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ is a row-intersecting code of dimension k, then

$$2\left\lfloor \frac{k-1}{m} \right\rfloor < n < 2m \qquad \text{and} \qquad \min_{A\in\mathcal{C}\setminus\{0\}} \mathrm{rk} A \geq \frac{k}{m}.$$

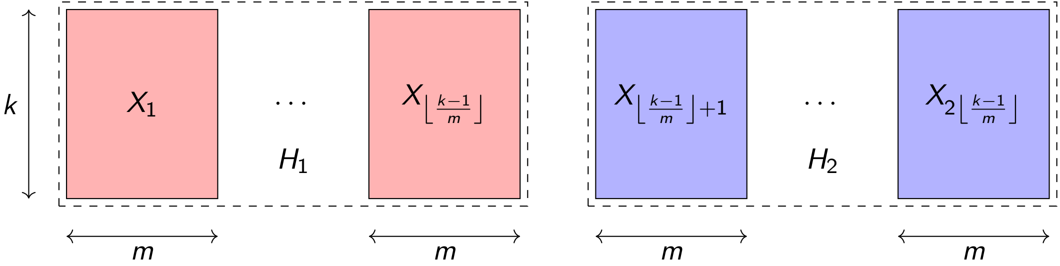
Bounds on parameters

Theorem

If $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ is a row-intersecting code of dimension k, then

$$2\left\lfloor \frac{k-1}{m} \right\rfloor < n < 2m \quad \text{and} \quad \min_{A\in\mathcal{C}\setminus\{0\}} \mathrm{rk} A \geq \frac{k}{m}.$$

Sketch of the proof:



Rank-metric case

Structural properties

Bounds on parameters

Geometric characterization

Constructions

Applications

$\cdots$

Contructions

Example

All $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ with $\min_{A\in\mathcal{C}\setminus\{0\}} \mathrm{rk}(A) > \frac{n}{2}$ are row-intersecting: known constructions of MRD codes (**Gabidulin codes** or their generalization).

Theorem

For $2 \leq h \leq \left\lfloor \frac{m+1}{2} \right\rfloor$, $\exists \mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ row-intersecting of dimension hm for

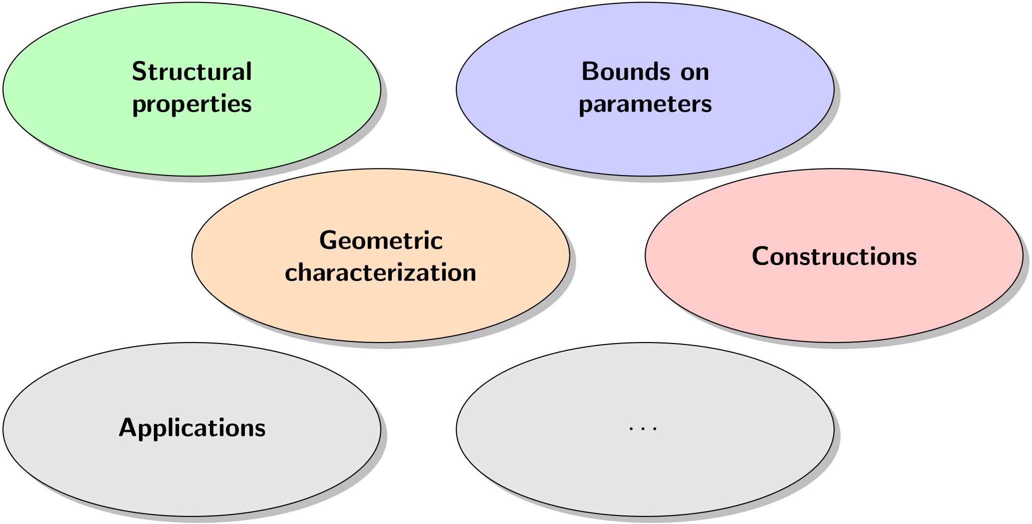
$$n \in \{m, \dots, 2m - 2h + 1\}.$$

Theorem (Vila, 2026+)

For $N \in \mathrm{GL}_n(\mathbb{F}_q)$,

$\mathcal{C} = \mathbb{F}_q[N]$ is row-intersecting $\iff$ N's minimal polynomial has 1 irreducible factor.

Conclusion and outlook



Conclusion and outlook

Structural properties

Better bounds on parameters ?

Geometric characterization

Other constructions ?

Applications ?

. . .

Conclusion and outlook

Structural properties

Better bounds on parameters ?

Geometric characterization

Other constructions ?

Applications ?

Thank you for your attention!