On the maximum weight codewords of linear rank-metric codes

Paolo Santonastaso
Università degli Studi della Campania "Luigi Vanvitelli"

Joint work with Olga Polverino and Ferdinando Zullo

WCC 2024: The Thirteenth International Workshop on Coding and Cryptography

Rank-metric codes

Rank-metric codes

$$\mathbb{F}_q^{m\times n}$$

Rank distance

$$d(A,B) = w(A-B) = \mathrm{Rank}(A-B)$$

(Linear) code: $\mathscr{C} \leq \mathbb{F}_q^{m\times n}$

Minimum distance:

$$d = d(\mathscr{C}) = \min\{d(A,B) : A, B \in \mathscr{C}, A \neq B\}$$

Singleton-like bound:

$$|\mathscr{C}| \leq q^{\max\{m,n\}(\min\{m,n\}-d+1)},$$

$= \rightarrow$ MRD-code

Rank-metric codes

$\mathbb{F}_q^{m\times n}$

Rank distance

$d(A,B) = w(A-B) = \mathrm{Rank}(A-B)$

(Linear) code: $\mathscr{C} \leq \mathbb{F}_q^{m\times n}$

Minimum distance:

$d = d(\mathscr{C}) = \min\{d(A,B) : A, B \in \mathscr{C}, A \neq B\}$

Singleton-like bound:

$|\mathscr{C}| \leq q^{\max\{m,n\}(\min\{m,n\}-d+1)}$,

$= \rightarrow$ **MRD-code**

* E. Gorla and A. Ravagnani: Codes endowed with the rank metric, Network Coding and Subspace Designs. Springer, Cham, 2018. 3-23.
* J. Sheekey: "13. MRD codes: constructions and connections". Combinatorics and Finite Fields: Difference Sets, Polynomials, Pseudorandomness and Applications, De Gruyter, 2019, 255-286.
* H. Bartz, L. Holzbaur, H. Liu, S. Puchinger, J. Renner and A. Wachter-Zeh, Rank-Metric Codes and Their Applications, Foundations and Trends® in Communications and Information Theory, 19(3) (2022), 390-546.

Rank-metric codes

$\mathbb{F}_q^{m\times n}$

Rank distance

$d(A,B) = w(A-B) = \mathrm{Rank}(A-B)$

(Linear) code: $\mathscr{C} \leq \mathbb{F}_q^{m\times n}$

Minimum distance:

$d = d(\mathscr{C}) = \min\{d(A,B) \colon A,B \in \mathscr{C}, A \neq B\}$

Singleton-like bound:

$|\mathscr{C}| \leq q^{\max\{m,n\}(\min\{m,n\}-d+1)}$,

$= \rightarrow$ MRD-code

Weight distribution of $\mathscr{C}$:

A_i= # codewords in $\mathscr{C}$ of (rank) weight i

$(A_0, A_1, \ldots, A_M)$

$M = \min\{m,n\}$

Rank-metric codes

$\mathbb{F}_q^{m\times n}$

Rank distance

$d(A,B) = w(A-B) = \mathrm{Rank}(A-B)$

(Linear) code: $\mathscr{C} \leq \mathbb{F}_q^{m\times n}$

Minimum distance:

$d = d(\mathscr{C}) = \min\{d(A,B) : A, B \in \mathscr{C}, A \neq B\}$

Singleton-like bound:

$|\mathscr{C}| \leq q^{\max\{m,n\}(\min\{m,n\}-d+1)}$,

$= \rightarrow$ MRD-code

Weight distribution of $\mathscr{C}$:

A_i= # codewords in $\mathscr{C}$ of (rank) weight i

$(A_0, A_1, \ldots, A_M)$

$M = \min\{m, n\}$

Rank-metric codes

$\mathbb{F}_q^{m\times n}$

Rank distance

$d(A,B) = w(A-B) = \mathrm{Rank}(A-B)$

(Linear) code: $\mathscr{C} \leq \mathbb{F}_q^{m\times n}$

Minimum distance:

$d = d(\mathscr{C}) = \min\{d(A,B) \colon A,B \in \mathscr{C}, A \neq B\}$

Singleton-like bound:

$|\mathscr{C}| \leq q^{\max\{m,n\}(\min\{m,n\}-d+1)}$,

$= \rightarrow$ MRD-code

Problem

Fixed n, m, q, k.

If $\mathscr{C} \leq \mathbb{F}_q^{m\times n}$ and $\dim_{\mathbb{F}_q}(\mathscr{C}) = k$

Bounds on

$M(\mathscr{C}) = A_{\min\{m,n\}}$

Rank-metric codes

Problem

Fixed n, m, q, k.

If $\mathscr{C} \leq \mathbb{F}_q^{m\times n}$ and $\dim_{\mathbb{F}_q}(\mathscr{C}) = k$

Bounds on

$$M(\mathscr{C}) = A_{\min\{m,n\}}$$

In the Hamming metric...

S. Ball and A. Blokhuis: A bound for the maximum weight of a linear code, SIAM Journal on Discrete Mathematics (2013)

Rank-metric codes

The weight distribution is uniquely determined for MRD codes!

Problem

Fixed n, m, q, k.

If $\mathscr{C} \leq \mathbb{F}_q^{m\times n}$ and $\dim_{\mathbb{F}_q}(\mathscr{C}) = k$

Bounds on

$$M(\mathscr{C}) = A_{\min\{m,n\}}$$

For MRD codes

$\mathscr{C}$ MRD code in $\mathbb{F}_q^{m\times n}$

$d(\mathscr{C}) = d$

$m' = \min\{m,n\}$ and $n' = \max\{m,n\}$

$$A_{d+\ell} = \begin{bmatrix} m' \\ d+\ell \end{bmatrix}_q \sum_{t=0}^{\ell} (-1)^{t-\ell} \begin{bmatrix} \ell+d \\ \ell-t \end{bmatrix}_q q^{\binom{\ell-t}{2}} (q^{n'(t+1)}-1)$$

for any $\ell \in \{0,1,\ldots,n'-d\}$

Linear rank-metric codes, q-systems and linear sets

Rank-metric codes

$$\mathbb{F}_{q^m}^n$$

Rank distance

$d(\mathbf{a},\mathbf{b}) = w(\mathbf{a}-\mathbf{b}) = \dim_{\mathbb{F}_q}(\langle a_1-b_1,\ldots,a_n-b_n\rangle_{\mathbb{F}_q})$

(Linear) code: $\mathscr{C} \leq \mathbb{F}_{q^m}^n$ $\quad [n,k]_{q^m/q}$ code

Minimum distance:

$d = d(\mathscr{C}) = \min\{d(\mathbf{a},\mathbf{b}) : \mathbf{a},\mathbf{b} \in \mathscr{C}, \mathbf{a} \neq \mathbf{b}\}$

Linear codes and q-systems

Sheekey-2019
Randrianarisoa-2020

$\mathscr{C} \leq \mathbb{F}_{q^m}^n$
non-degenerate linear code
$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k$

$G = \left(\mathbf{g}_1 \cdots \mathbf{g}_n\right) \in \mathbb{F}_{q^m}^{k\times n}$

$U = \langle \mathbf{g}_1^t, \ldots, \mathbf{g}_n^t \rangle_{\mathbb{F}_q} \subseteq \mathbb{F}_{q^m}^k$
q-system

$$w(xG) = n - \dim_{\mathbb{F}_q}(U \cap x^{\perp})$$

$$n - d(\mathscr{C}) = \max\{\dim_{\mathbb{F}_q}(H \cap U) \colon H \subset \mathbb{F}_{q^m}^k, \dim(H) = k-1\}$$

Linear codes and q-systems

Sheekey-2019

Randrianarisoa-2020

$\mathscr{C} \leq \mathbb{F}_{q^m}^n$

non-degenerate linear code

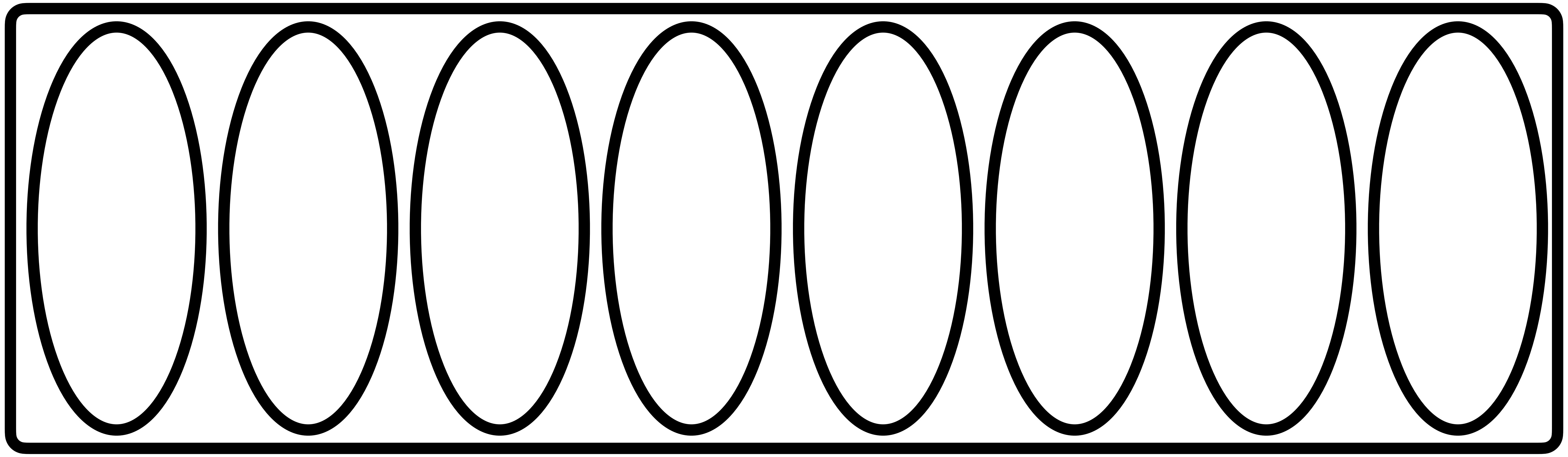
$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k$

$G = \left(\mathbf{g}_1 \cdots \mathbf{g}_n\right) \in \mathbb{F}_{q^m}^{k\times n}$

$U = \langle \mathbf{g}_1^t, \ldots, \mathbf{g}_n^t \rangle_{\mathbb{F}_q} \subseteq \mathbb{F}_{q^m}^k$

$L_U = \{\langle u \rangle_{\mathbb{F}_{q^m}} : u \in U \setminus \{0\}\} \subseteq \mathrm{PG}(k-1, q^m)$ $\mathbb{F}_q$-linear set

$w_{L_U}(\Lambda) = \dim_{\mathbb{F}_q}(U \cap W)$ Weight of $\Lambda = \mathrm{PG}(W, \mathbb{F}_{q^m})$



$\mathrm{PG}(k-1, q^m)$

Linear codes and q-systems

Sheekey-2019

Randrianarisoa-2020

$\mathscr{C} \leq \mathbb{F}_{q^m}^n$

non-degenerate linear code

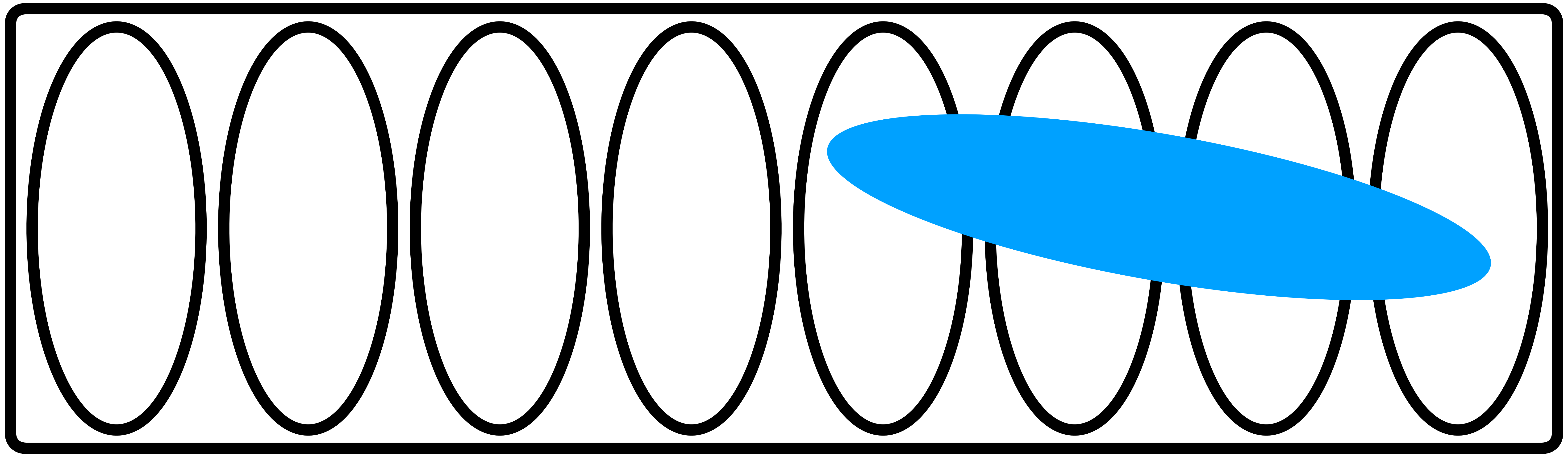
$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k$

$G = \left(\mathbf{g}_1 \cdots \mathbf{g}_n\right) \in \mathbb{F}_{q^m}^{k \times n}$

$U = \langle \mathbf{g}_1^t, \ldots, \mathbf{g}_n^t \rangle_{\mathbb{F}_q} \subseteq \mathbb{F}_{q^m}^k$

$L_U = \{\langle u \rangle_{\mathbb{F}_{q^m}} : u \in U \setminus \{0\}\} \subseteq \mathrm{PG}(k-1, q^m)$ $\mathbb{F}_q$-linear set

$w_{L_U}(\Lambda) = \dim_{\mathbb{F}_q}(U \cap W)$ Weight of $\Lambda = \mathrm{PG}(W, \mathbb{F}_{q^m})$



$\mathrm{PG}(k-1, q^m)$

L_U

Linear codes and q-systems

Sheekey-2019

Randrianarisoa-2020

$\mathscr{C} \leq \mathbb{F}_{q^m}^n$

non-degenerate linear code

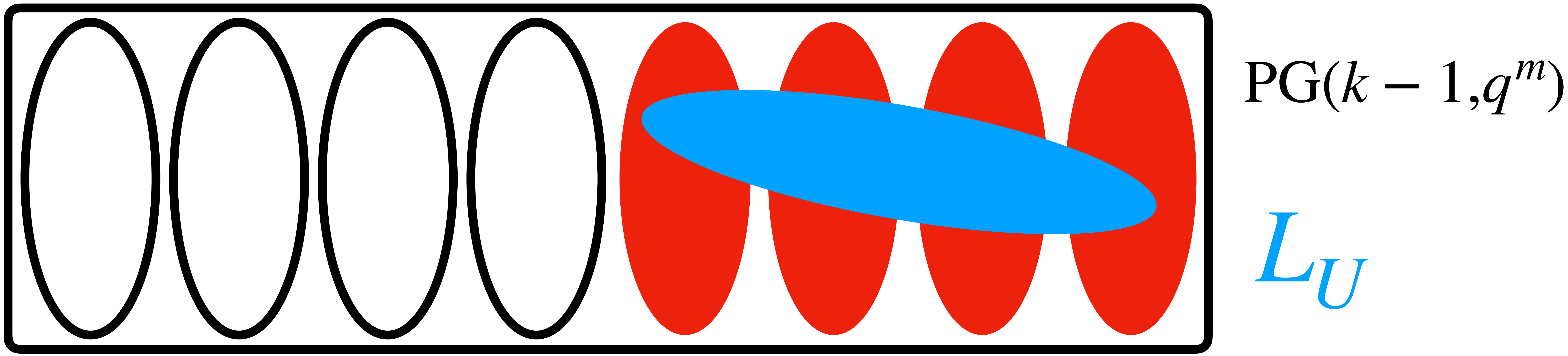
$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k$

$G = \left(\mathbf{g}_1 \cdots \mathbf{g}_n\right) \in \mathbb{F}_{q^m}^{k \times n}$

$U = \langle \mathbf{g}_1^t, \ldots, \mathbf{g}_n^t \rangle_{\mathbb{F}_q} \subseteq \mathbb{F}_{q^m}^k$

$L_U = \{\langle u \rangle_{\mathbb{F}_{q^m}} : u \in U \setminus \{0\}\} \subseteq \mathrm{PG}(k-1, q^m)$ $\mathbb{F}_q$-linear set

$w_{L_U}(\Lambda) = \dim_{\mathbb{F}_q}(U \cap W)$ Weight of $\Lambda = \mathrm{PG}(W, \mathbb{F}_{q^m})$



Linear codes and q-systems

Sheekey-2019

Randrianarisoa-2020

$\mathscr{C} \leq \mathbb{F}_{q^m}^n$

non-degenerate linear code

$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k$

$G = \left(\mathbf{g}_1 \cdots \mathbf{g}_n\right) \in \mathbb{F}_{q^m}^{k \times n}$

$U = \langle \mathbf{g}_1^t, \ldots, \mathbf{g}_n^t \rangle_{\mathbb{F}_q} \subseteq \mathbb{F}_{q^m}^k$

$L_U = \{\langle u \rangle_{\mathbb{F}_{q^m}} : u \in U \setminus \{0\}\} \subseteq \mathrm{PG}(k-1, q^m)$ $\mathbb{F}_q$-linear set

$w_{L_U}(\Lambda) = \dim_{\mathbb{F}_q}(U \cap W)$ Weight of $\Lambda = \mathrm{PG}(W, \mathbb{F}_{q^m})$

Weight distribution of $\mathscr{C}$ ⟷ Hyperplanes weight distribution of L_U

Linear codes and q-systems

$\mathscr{C} \leq \mathbb{F}_{q^m}^n$

non-degenerate linear code

$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k$

$G = \left(\mathbf{g}_1 \cdots \mathbf{g}_n\right) \in \mathbb{F}_{q^m}^{k \times n}$

Problem

Fixed n, m, q, k.

If $\mathscr{C} \leq \mathbb{F}_{q^m}^n$ and $\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k$

⇓

Bounds on

$M(\mathscr{C}) = A_{\min\{m,n\}}$

Linear codes and q-systems

$\mathscr{C} \leq \mathbb{F}_{q^m}^n$

non-degenerate linear code

$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k$

$G = \left(\mathbf{g}_1 \cdots \mathbf{g}_n\right) \in \mathbb{F}_{q^m}^{k \times n}$

Alfarano, Borello, Neri and Ravagnani 2021

$\mathscr{C}$ is non degenerate $\Leftrightarrow M(\mathscr{C}) \geq 1$

Problem

Fixed n, m, q, k.

If $\mathscr{C} \leq \mathbb{F}_{q^m}^n$ and $\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k$

⇓

Bounds on

$M(\mathscr{C}) = A_{\min\{m,n\}}$

Dimension two case

$$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = 2$$

$\mathscr{C} \leq \mathbb{F}_{q^m}^n$

non-degenerate linear code

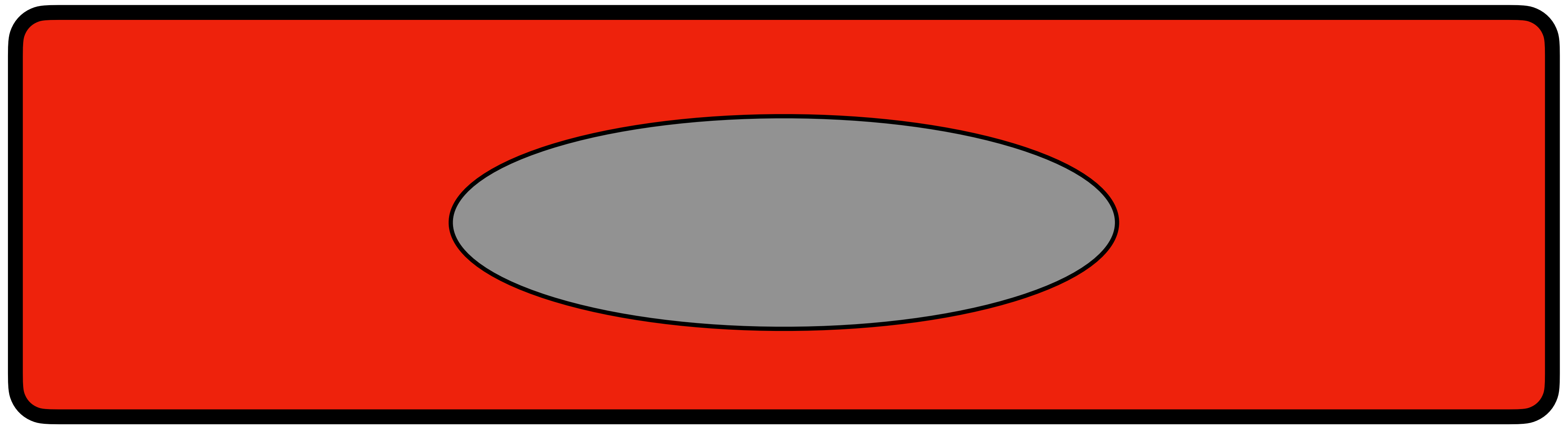
$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = 2$

$G = \left(\mathbf{g}_1 \cdots \mathbf{g}_n\right) \in \mathbb{F}_{q^m}^{2\times n}$

$U = \langle \mathbf{g}_1^t, \ldots, \mathbf{g}_n^t \rangle_{\mathbb{F}_q} \subseteq \mathbb{F}_{q^m}^2$

$$n \leq m$$

PG(1,q^m)



L_U

$M(\mathscr{C}) = (q^m - 1)\,|\mathrm{PG}(1,q^m) \backslash L_U|$

$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = 2$

$\mathscr{C} \leq \mathbb{F}_{q^m}^n$

non-degenerate linear code

$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = 2$

$G = \left(\mathbf{g}_1 \cdots \mathbf{g}_n\right) \in \mathbb{F}_{q^m}^{2\times n}$

$U = \langle \mathbf{g}_1^t, \ldots, \mathbf{g}_n^t \rangle_{\mathbb{F}_q} \subseteq \mathbb{F}_{q^m}^2$

$n \leq m$

Bounds on $M(\mathscr{C})$

Bounds on $|L_U|$

$M(\mathscr{C}) = (q^m - 1)\,|\mathrm{PG}(1,q^m) \setminus L_U|$

$$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = 2$$

$$n \leq m$$

$$M(\mathscr{C}) = (q^m - 1)\,|\,\mathrm{PG}(1,q^m)\backslash L_U\,|$$

$$q + 1 \leq |L_U| \leq \frac{q^n - 1}{q - 1}$$

$$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = 2$$

$$n \leq m$$

$$M(\mathscr{C}) = (q^m - 1)\,|\,\mathrm{PG}(1,q^m) \setminus L_U\,|$$

Subline $$q + 1 \leq |L_U| \leq \frac{q^n - 1}{q - 1}$$ Scattered linear set

$$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = 2$$

$$n \leq m$$

$$M(\mathscr{C}) = (q^m - 1)\,|\mathrm{PG}(1,q^m)\setminus L_U|$$

Subline $\quad q + 1 \leq |L_U| \leq \dfrac{q^n - 1}{q - 1} \quad$ Scattered linear set

$$q^{2m} - 1 - (q^m - 1)\frac{q^n - 1}{q - 1} \leq M(\mathscr{C}) \leq q^{2m} - 1 - (q^m - 1)(q + 1)$$

$$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = 2$$

$$n \leq m$$

$$M(\mathscr{C}) = (q^m - 1)\,|\mathrm{PG}(1,q^m)\setminus L_U|$$

If $A_{n-1} > 0$

De Beule and Van de Voorde - 2019

If $w_{L_U}(P) = 1 \Rightarrow \quad |L_U| \geq q^{n-1} + 1$

$$q^{2m} - 1 - (q^m - 1)\frac{q^n - 1}{q - 1} \leq M(\mathscr{C}) \leq q^{2m} - 1 - (q^m - 1)(q^{n-1} + 1)$$

$$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = 2$$

$$n \leq m$$

$$M(\mathscr{C}) = (q^m - 1)\,|\mathrm{PG}(1,q^m)\backslash L_U|$$

If $n - e$ = second maximum weight of $\mathscr{C}$

$$q^{2m} - 1 - (q^m - 1)\frac{q^n - 1}{q^e - 1} \leq M(\mathscr{C}) \leq q^{2m} - 1 - (q^m - 1)(q^{n-e} + 1)$$

Adriaensen and PS - 2023 + De Beule and Van de Voorde - 2019

$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = 2$

$n \leq m$

$M(\mathscr{C}) = (q^m - 1)\,|\mathrm{PG}(1,q^m) \setminus L_U|$

If $n - e$ = second maximum weight of $\mathscr{C}$

$$q^{2m} - 1 - (q^m - 1)\frac{q^n - 1}{q^e - 1} \leq M(\mathscr{C}) \leq q^{2m} - 1 - (q^m - 1)(q^{n-e} + 1)$$

Adriaensen and
PS - 2023

+

De
Vo

$$e = n - \left\lfloor \log_q\left(q^m + 1 - \frac{M(\mathscr{C})}{q^m - 1}\right)\right\rfloor$$

$$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = 2$$

$$n \leq m$$

$$M(\mathscr{C}) = (q^m - 1)\,|\,\mathrm{PG}(1,q^m)\setminus L_U\,|$$

If $n-e$ = second maximum weight of $\mathscr{C}$ and $m=n$

$$q^{2m} - 1 - (q^m - 1)\frac{q^n - 1}{q^e - 1} \leq M(\mathscr{C})$$

O. Polverino, PS, J. Sheekey and F. Zullo: Divisible linear rank metric codes (2023)

Adriae… e Beule and Van de

PS - 2… oorde - 2019

$e \mid m$ and $\mathscr{C}$ is e-divisible

$$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = 2$$

$\mathscr{C} \leq \mathbb{F}_{q^m}^n$

non-degenerate linear code

$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = 2$

$G = \left(\mathbf{g}_1 \cdots \mathbf{g}_n\right) \in \mathbb{F}_{q^m}^{2\times n}$

$U = \langle \mathbf{g}_1^t, \ldots, \mathbf{g}_n^t \rangle_{\mathbb{F}_q} \subseteq \mathbb{F}_{q^m}^2$

$n > m$

$$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = 2$$

$\mathscr{C} \leq \mathbb{F}_{q^m}^n$

non-degenerate linear code

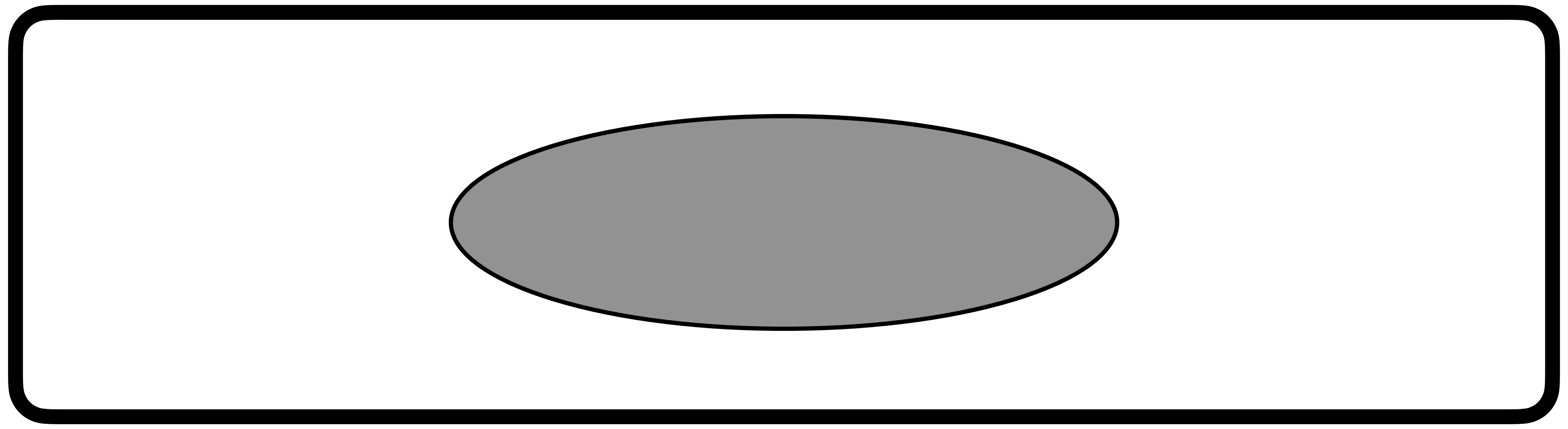
$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = 2$

$G = \left(\mathbf{g}_1 \cdots \mathbf{g}_n\right) \in \mathbb{F}_{q^m}^{2\times n}$

$U = \langle \mathbf{g}_1^t, \ldots, \mathbf{g}_n^t \rangle_{\mathbb{F}_q} \subseteq \mathbb{F}_{q^m}^2$

$n > m$

$\mathrm{PG}(1,q^m)$



L_U

$$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = 2$$

$\mathscr{C} \leq \mathbb{F}_{q^m}^n$

non-degenerate linear code

$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = 2$

$G = \left(\mathbf{g}_1 \cdots \mathbf{g}_n\right) \in \mathbb{F}_{q^m}^{2\times n}$

$U = \langle \mathbf{g}_1^t, \ldots, \mathbf{g}_n^t \rangle_{\mathbb{F}_q} \subseteq \mathbb{F}_{q^m}^2$

$\sigma \colon \mathbb{F}_{q^m}^k \times \mathbb{F}_{q^m}^k \to \mathbb{F}_{q^m}$

Nondegenerate reflexive bilinear form

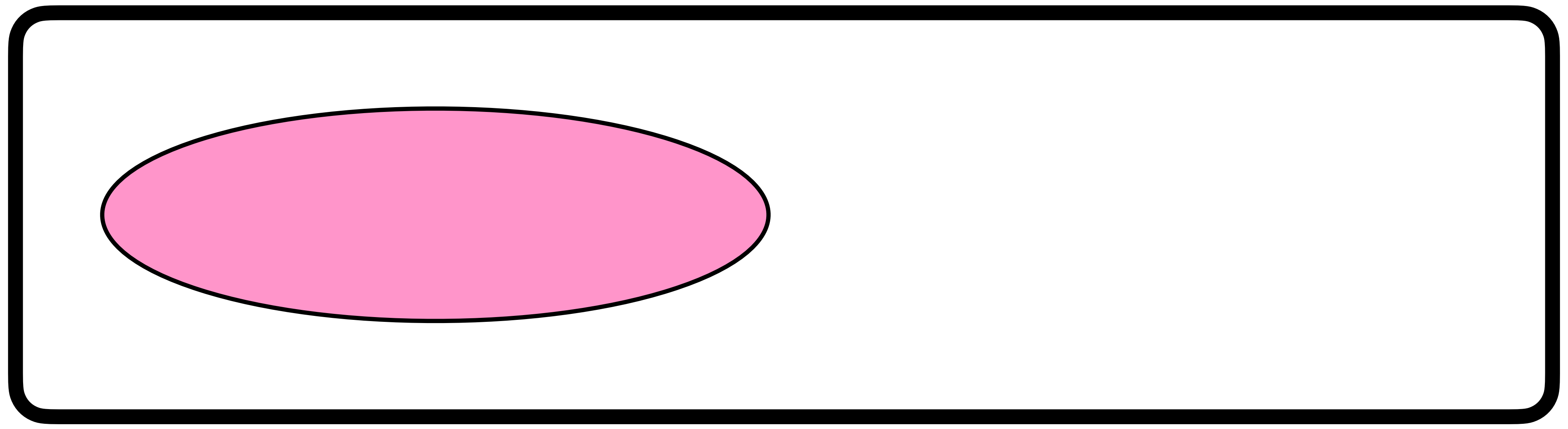
$\sigma' = \mathrm{Tr}_{q^m/q} \circ \sigma \colon \mathbb{F}_{q^m}^k \times \mathbb{F}_{q^m}^k \to \mathbb{F}_q$

Nondegenerate reflexive bilinear form

$\perp \to$ orthogonal complement

$$n > m$$

PG(1,q^m)



$L_{U^\perp}$

$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = 2$

$\mathscr{C} \leq \mathbb{F}_{q^m}^n$

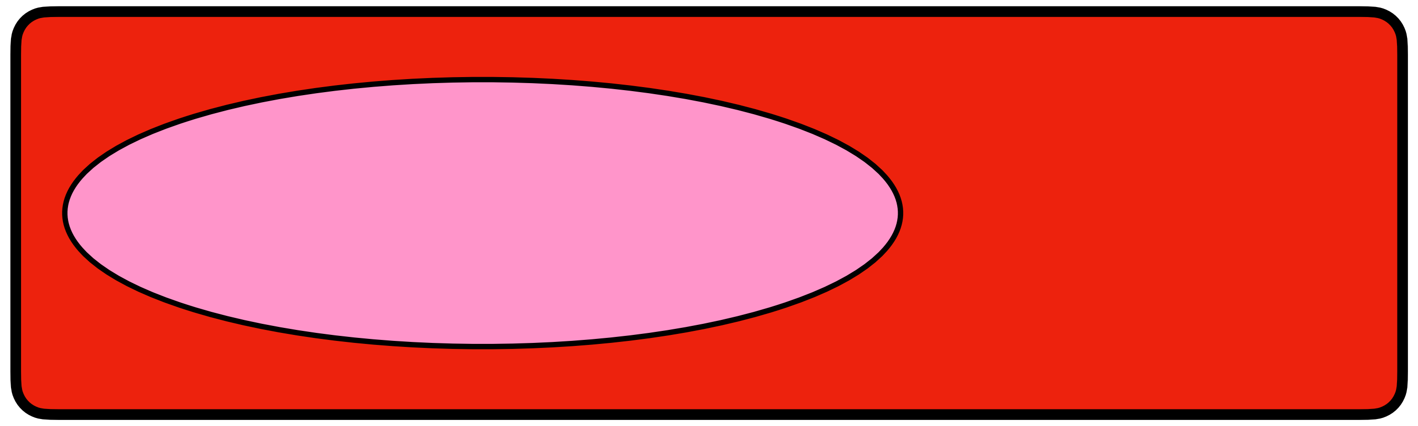
non-degenerate linear code

$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = 2$

$G = \left(\mathbf{g}_1 \cdots \mathbf{g}_n\right) \in \mathbb{F}_{q^m}^{2\times n}$

$U = \langle \mathbf{g}_1^t, \ldots, \mathbf{g}_n^t \rangle_{\mathbb{F}_q} \subseteq \mathbb{F}_{q^m}^2$

$n > m$



$\mathrm{PG}(1,q^m)$

$L_{U^\perp}$

$M(\mathscr{C}) = (q^m - 1)\,|\,\mathrm{PG}(1,q^m) \setminus L_{U^\perp}\,|$

$\sigma\colon \mathbb{F}_{q^m}^k \times \mathbb{F}_{q^m}^k \to \mathbb{F}_{q^m}$

Nondegenerate reflexive bilinear form

$\sigma' = \mathrm{Tr}_{q^m/q} \circ \sigma\colon \mathbb{F}_{q^m}^k \times \mathbb{F}_{q^m}^k \to \mathbb{F}_q$

Nondegenerate reflexive bilinear form

$\perp \to$ orthogonal complement

$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = 2$

$n > m$

$M(\mathscr{C}) = (q^m - 1)\,|\,\mathrm{PG}(1,q^m)\setminus L_{U^\perp}\,|$

$$q^{2m} - 1 - (q^m - 1)\frac{q^{2m-n} - 1}{q - 1} \leq M(\mathscr{C}) \leq q^{2m} - 1 - (q^m - 1)(q + 1)$$

If $n - e$ = second maximum weight of $\mathscr{C}$

$$q^{2m} - 1 - (q^m - 1)\frac{q^{2m-n} - 1}{q^e - 1} \leq M(\mathscr{C}) \leq q^{2m} - 1 - (q^m - 1)(q^{2m-n-e} + 1)$$

$$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = 2$$

$$n > m$$

$$M(\mathscr{C}) = (q^m - 1)\,|\,\mathrm{PG}(1,q^m)\setminus L_{U^\perp}\,|$$

$$q^{2m} - 1 - (q^m - 1)\frac{q^{2m-n} - 1}{q - 1} \leq M(\mathscr{C}) \leq q^{2m} - 1 - (q^m - 1)(q + 1)$$

If $n - e$ = second maximum weight of $\mathscr{C}$

$$q^{2m} - 1 - (q^m - 1)\frac{q^{2m-n} - 1}{q^e - 1} \leq M$$

$$e = 2m - \left\lfloor \log_q \left(q^m + 1 - \frac{M(\mathscr{C})}{q^m - 1} \right) \right\rfloor - n$$

Tightness of the bounds

$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = 2$ and $d(\mathscr{C}) \geq n - m + 1$

$M(\mathscr{C})$ is minimum ⟺ $\mathscr{C}$ or $\mathscr{C}^{\perp_{\mathcal{G}}}$ is an MRD code

$M(\mathscr{C})$ is maximum ⟺ $n = k = 2$ and either $\mathscr{C}$ or $\mathscr{C}^{\perp_{\mathcal{G}}}$ is $\mathbb{F}_{q^m}^2$

If $A_{n-1} > 0$

$M(\mathscr{C})$ is maximum ⟺ Either L_U or $L_{U^\perp}$ is minimum size

Geometric dual of rank-metric codes

$[\mathscr{C}] \in \mathfrak{C}[n,k]_{q^m/q}$

↓

$[U] \in \mathfrak{U}[n,k]_{q^m/q}$

↓

$[U^\perp] \in \mathfrak{U}[mk-n,k]_{q^m/q}$

↓

$[\mathscr{C}^{\perp_{\mathcal{G}}}] \in \mathfrak{C}[km-n,k]_{q^m/q}$

$\sigma\colon \mathbb{F}_{q^m}^k \times \mathbb{F}_{q^m}^k \to \mathbb{F}_{q^m}$
Nondegenerate reflexive bilinear form

$\sigma' = \mathrm{Tr}_{q^m/q} \circ \sigma\colon \mathbb{F}_{q^m}^k \times \mathbb{F}_{q^m}^k \to \mathbb{F}_q$
Nondegenerate reflexive bilinear form

$\perp \to$ orthogonal complement

Borello and Zullo: Geometric dual and sum-rank minimal codes (2023)

Larger dimension..

$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k$ $\quad n \leq m$

$\mathscr{C} \leq \mathbb{F}_{q^m}^n$

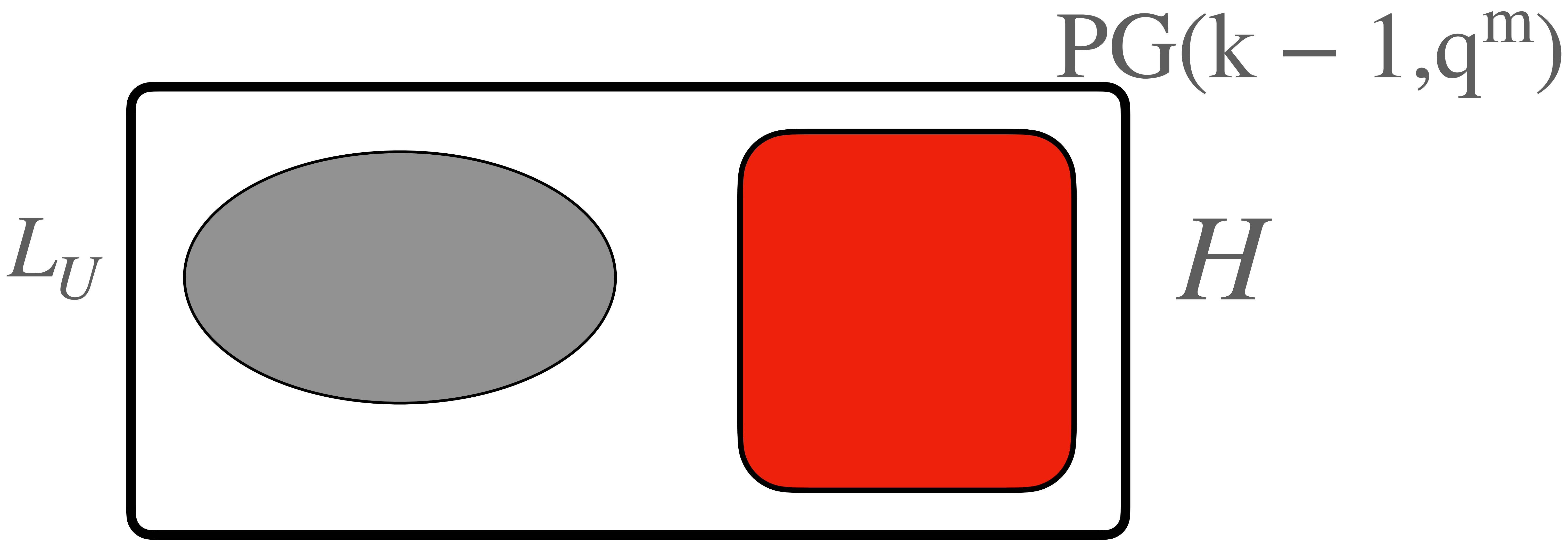
non-degenerate linear code

$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k$

$G = (\mathbf{g}_1 \cdots \mathbf{g}_n) \in \mathbb{F}_{q^m}^{k \times n}$

$U = \langle \mathbf{g}_1^t, \ldots, \mathbf{g}_n^t \rangle_{\mathbb{F}_q} \subseteq \mathbb{F}_{q^m}^k$

$M(\mathscr{C}) = (q^m - 1) \,|\, \{H = \mathrm{PG}(k-2, q^m) : H \cap L_U = \varnothing\} \,|$

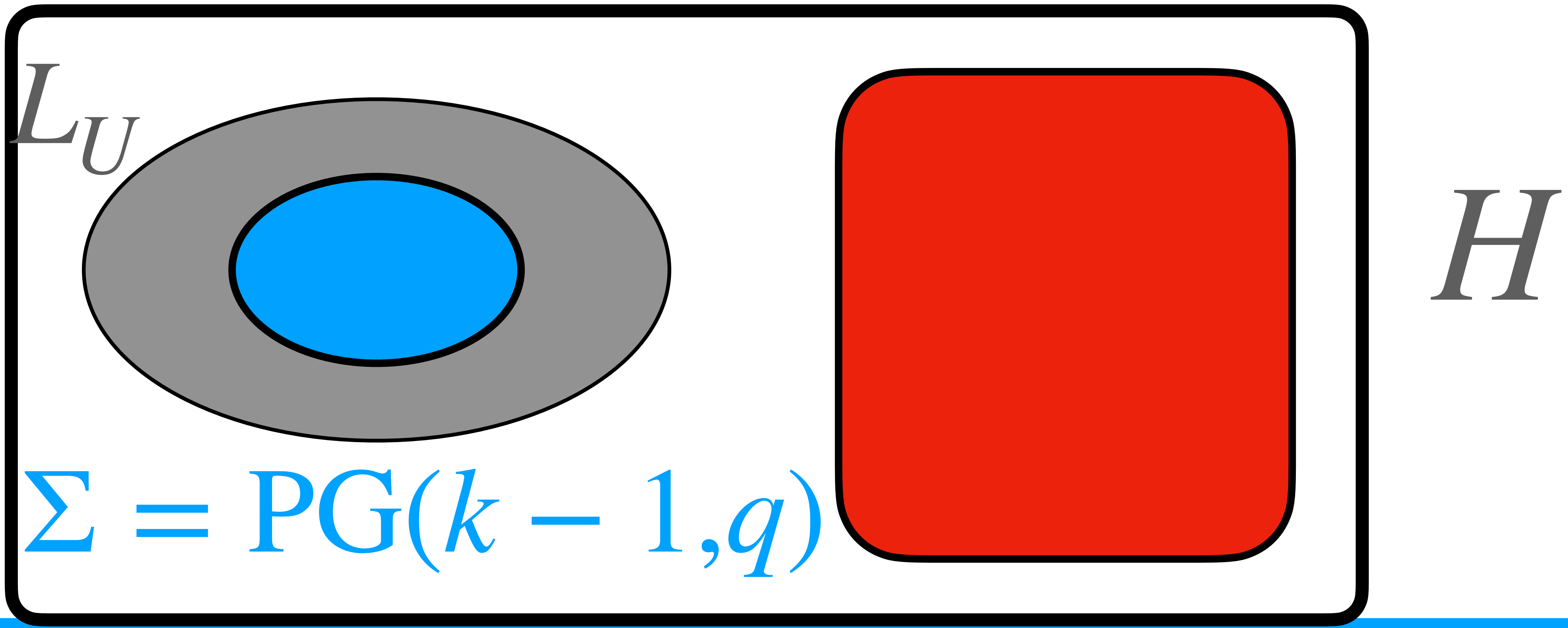


$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k$ $\quad n \leq m$

$$M(\mathscr{C}) = (q^m - 1)\,|\,\{H = \mathrm{PG}(k-2, q^m) : H \cap L_U = \emptyset\}\,|$$

$$\frac{q^{mk}-1}{q^m-1} - \frac{q^n-1}{q-1}\frac{q^{(k-1)m}-1}{q^m-1} + q\beta \leq \frac{M(\mathscr{C})}{q^m-1} \leq \prod_{i=1}^{n-1}(q^m - q^i)$$

β = #secant hyperplanes to Σ



Number of rank n matrices in $\mathbb{F}_q^{m\times n}$

$$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k$$

$$n \leq m$$

$$M(\mathscr{C}) = (q^m - 1)\,|\,\{H = \mathrm{PG}(k-2, q^m) : H \cap L_U = \varnothing\}\,|$$

If $n - e$ = second maximum weight of $\mathscr{C}$

$$q^{m(k-1)} - q^{m(k-2)+n-e} - q^{m(k-2)}\left(\frac{q^{n-e}-1}{q^e-1}\right) \leq \frac{M(\mathscr{C})}{q^m-1} \leq q^{m(k-1)} - q^{m(k-2)+n-e}$$

$$e = n - \left\lfloor \log_q\left(q^{m(k-1)} - \frac{M(\mathscr{C})}{q^m-1}\right)\right\rfloor + m(k-2)$$

$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k$ $n > m$

$\mathscr{C} \leq \mathbb{F}_{q^m}^n$

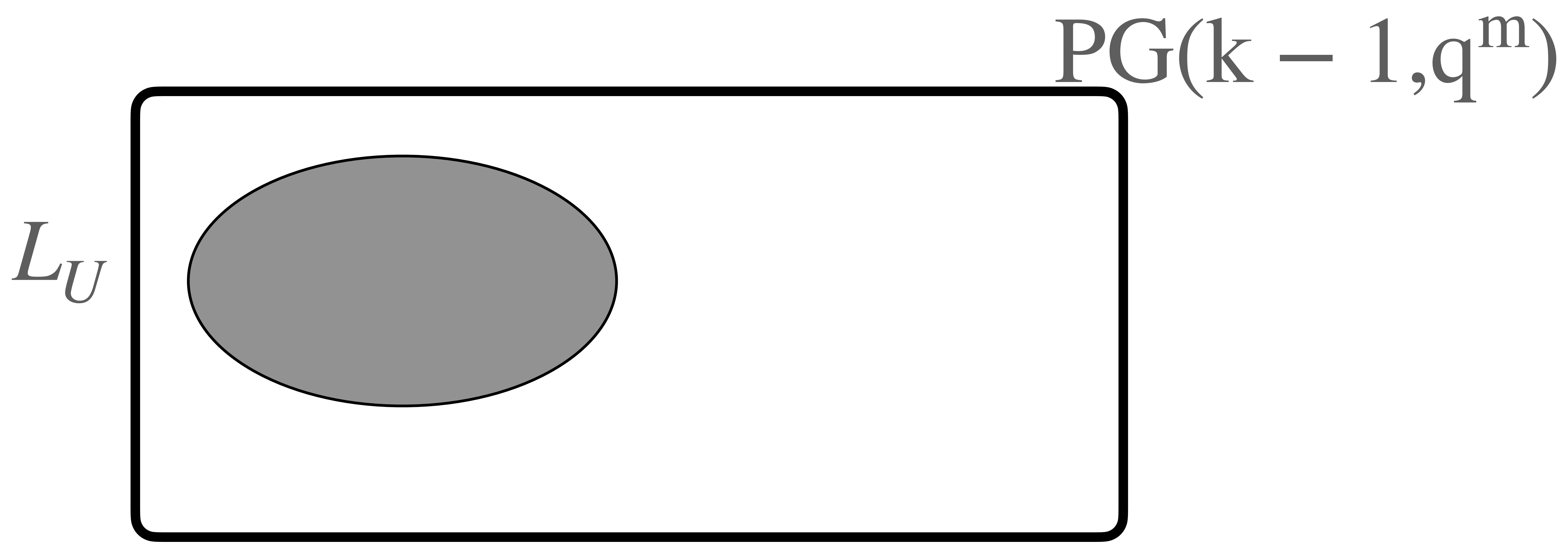
non-degenerate linear code

$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k$

$G = \left(\mathbf{g}_1 \cdots \mathbf{g}_n\right) \in \mathbb{F}_{q^m}^{k \times n}$

$U = \langle \mathbf{g}_1^t, \ldots, \mathbf{g}_n^t \rangle_{\mathbb{F}_q} \subseteq \mathbb{F}_{q^m}^k$

$M(\mathscr{C}) = (q^m - 1)\,|\,\mathrm{PG}(k-1, q^m) \setminus L_{U^\perp}\,|$



$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k$ $n > m$

$\mathscr{C} \leq \mathbb{F}_{q^m}^n$

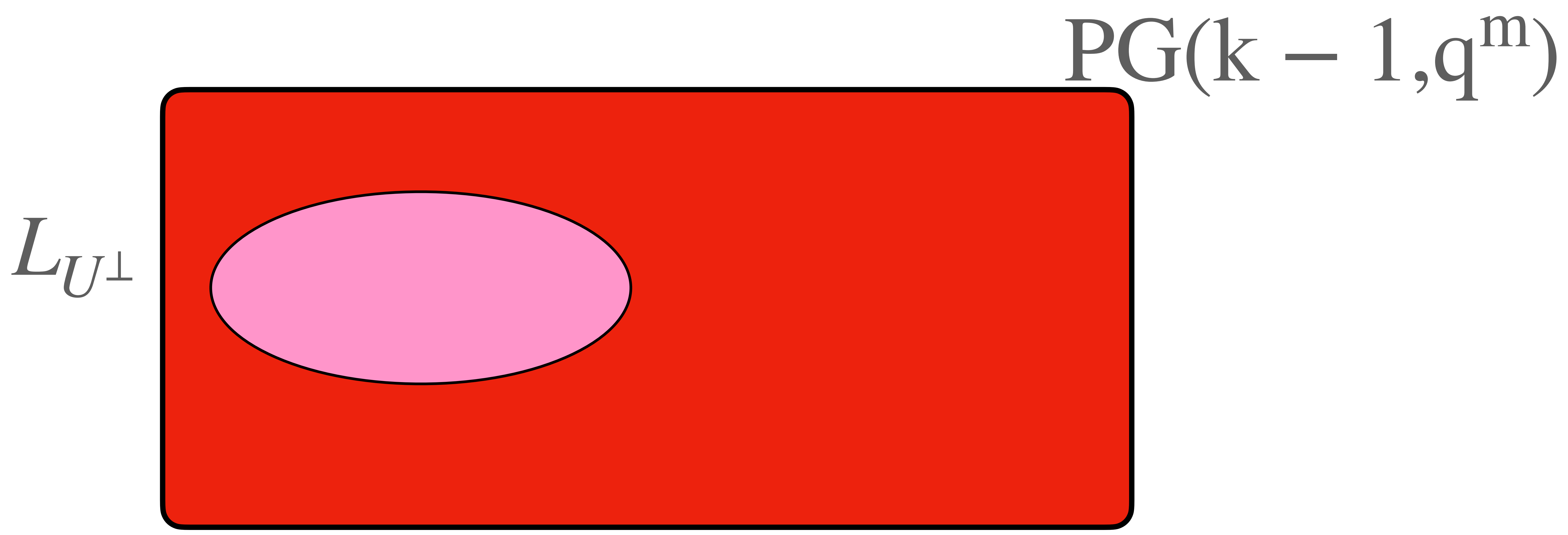
non-degenerate linear code

$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k$

$G = \left(\mathbf{g}_1 \cdots \mathbf{g}_n\right) \in \mathbb{F}_{q^m}^{k \times n}$

$U = \langle \mathbf{g}_1^t, \ldots, \mathbf{g}_n^t \rangle_{\mathbb{F}_q} \subseteq \mathbb{F}_{q^m}^k$

$M(\mathscr{C}) = (q^m - 1)\,|\,\mathrm{PG}(k-1, q^m) \setminus L_{U^\perp}\,|$



$$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k \qquad n > m$$

$$M(\mathscr{C}) = (q^m - 1)\,|\mathrm{PG}(k-1, q^m) \setminus L_{U^\perp}|$$

$$\frac{q^{mk}-1}{q^m-1} - \frac{q^{km-n}-1}{q-1} \leq \frac{M(\mathscr{C})}{q^m-1} \leq \frac{q^{mk}-1}{q^m-1} - \frac{q^k-1}{q-1}$$

$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k$ $n > m$

$$M(\mathscr{C}) = (q^m - 1)\,|\,\mathrm{PG}(k-1, q^m) \setminus L_{U^\perp}\,|$$

If $n - e$ = second maximum weight of $\mathscr{C}$

$$\frac{q^{mk}-1}{q^m-1} - \frac{q^{km-n}-1}{q-1} \leq \frac{M(\mathscr{C})}{q^m-1} \leq \frac{q^{mk}-1}{q^m-1} - \left(q^{km-n-e} + \frac{q^{k-1}-1}{q-1}\right)$$

Adriaensen and PS - 2023

$$e = mk - \left\lfloor \log_q\left(\frac{q^{mk}-1}{q^m-1} - \frac{M(\mathscr{C})}{q^m-1}\right)\right\rfloor - n$$

Equalities in the lower bounds...

$$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k$$

$$(q^{mk}-1) - \frac{q^n-1}{q-1}(q^{(k-1)m}-1) + q(q^m-1)\beta \leq M(\mathscr{C})$$

$$n < m$$

$$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k$$

$$(q^{mk}-1) - \frac{q^n-1}{q-1}(q^{(k-1)m}-1) + q(q^m-1)\beta = M(\mathscr{C})$$

$n < m$

$n = k$ and $\mathscr{C} = \mathbb{F}_{q^m}^k$

$$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k$$

$$q^{km} - 1 - (q^m - 1)\frac{q^{km-n} - 1}{q - 1} \leq M(\mathscr{C})$$

$$n \geq m$$

$$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k$$

$$q^{km} - 1 - (q^m - 1)\frac{q^{km-n} - 1}{q - 1} = M(\mathscr{C})$$

$$n \geq m$$

⇕

$L_{U^\perp}$ is scattered

$$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k$$

$$q^{km} - 1 - (q^m - 1)\frac{q^{km-n} - 1}{q - 1} = M(\mathscr{C})$$

$n \geq m$

⇕

$L_{U^\perp}$ is scattered

$n \geq km/2$

$$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k$$

$$q^{km} - 1 - (q^m - 1)\frac{q^{km-n} - 1}{q - 1} = M(\mathscr{C})$$

$n \geq m$

$M(\mathscr{C})$ is minimum ⟺ $L_{U^\perp}$ is scattered

$\mathscr{C}$ is MRD ⟺ $n = km/2$

$$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k$$

$$q^{km} - 1 - (q^m - 1)\frac{q^{km-n} - 1}{q - 1} = M(\mathscr{C})$$

$n \geq m$

$M(\mathscr{C})$ is minimum ⟺ $L_{U^\perp}$ is scattered

$\mathscr{C}$ is MRD ⟺ $n = km/2$

$U = \{(x, x^q, a) : x \in \mathbb{F}_{q^m}, a \in \mathbb{F}_q\}$
$W = U^\perp$
$\mathscr{C} \to W$

$M(\mathscr{C})$ is minimum,
$\mathscr{C}$ and $\mathscr{C}^{\perp_\mathscr{G}}$ is not MRD

Equalities on the upper bounds

$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k \qquad d_{k-1}^{\mathrm{rk}}(\mathscr{C}) \geq n - m + 1$

$$M(\mathscr{C}) \leq \prod_{i=0}^{n-1} (q^m - q^i)$$

$n < m$

$$M(\mathscr{C}) \leq q^{km} - 1 - (q^m - 1)\frac{q^k - 1}{q - 1}$$

$n \geq m$

$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k \qquad d^{\mathrm{rk}}_{k-1}(\mathscr{C}) \geq n - m + 1$

$$M(\mathscr{C}) = \prod_{i=0}^{n-1}(q^m - q^i)$$

$n < m$

$$M(\mathscr{C}) = q^{km} - 1 - (q^m - 1)\frac{q^k - 1}{q - 1}$$

$n \geq m$

Either $\mathscr{C} = \mathbb{F}_{q^m}^k$ or

$\mathscr{C} = \mathscr{C}_1 \oplus \cdots \oplus \mathscr{C}_k$, $\mathscr{C}_i$ is an $[m-1,1]_{q^m/q}$-code

$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k$ $n > m$

$W = \psi_{G'}\left(\mathrm{supp}(c)^{\perp *}\right)$ $\dim_{\mathbb{F}_q}(W) = \dim_{\mathbb{F}_{q^m}}(\langle W \rangle_{\mathbb{F}_{q^m}}) = k - 1$

$$M(\mathscr{C}) \leq q^{km} - 1 - (q^m - 1)\left(q^{km-n} + \ldots + q^{km-n-k+1} + 1\right)$$

$$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k \qquad n > m$$

$$W = \psi_{G'}\left(\mathrm{supp}(c)^{\perp *}\right) \qquad \dim_{\mathbb{F}_q}(W) = \dim_{\mathbb{F}_{q^m}}(\langle W \rangle_{\mathbb{F}_{q^m}}) = k - 1$$

$$M(\mathscr{C}) = q^{km} - 1 - (q^m - 1)\left(q^{km-n} + \ldots + q^{km-n-k+1} + 1\right)$$

$\lambda \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q$

$$G = \begin{pmatrix} 1 & \lambda & \ldots & \lambda^{t_1-1} & 0 & \ldots & & & & & & 0 \\ 0 & 0 & \ldots & 0 & 1 & \lambda & \ldots & \lambda^{t_2-1} & 0 & \ldots & & 0 \\ \vdots & & & & & & & & \ddots & & & \\ 0 & \ldots & & & & & & & 0 & 1 & \ldots & \lambda^{t_k-1} \end{pmatrix} \in \mathbb{F}_{q^m}^{k \times (t_1 + \ldots + t_k)}$$

$$\mathscr{C}_{\lambda, t_1, \ldots, t_k}$$

$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k$

$n > m$

$\lambda \in \mathbb{F}_{q^m} \backslash \mathbb{F}_q$

$$G = \begin{pmatrix} 1 & \lambda & \dots & \lambda^{t_1-1} & 0 & \dots & & & & & & 0 \\ 0 & 0 & \dots & 0 & 1 & \lambda & \dots & \lambda^{t_2-1} & 0 & \dots & & 0 \\ \vdots & & & & & & & & \ddots & & & \\ 0 & \dots & & & & & & & 0 & 1 & \dots & \lambda^{t_k-1} \end{pmatrix} \in \mathbb{F}_{q^m}^{k \times (t_1 + \dots + t_k)}$$

$$\mathscr{C}_{\lambda, t_1, \dots, t_k} = \mathscr{C}_{\lambda, t_1} \oplus \cdots \oplus \mathscr{C}_{\lambda, t_k}$$

1-dimensional MRD codes

$$\dim_{\mathbb{F}_{q^m}}(\mathscr{C}) = k \qquad n > m$$

$$\lambda \in \mathbb{F}_{q^m} \setminus \mathbb{F}_q$$

$$G = \begin{pmatrix} 1 & \lambda & \dots & \lambda^{t_1-1} & 0 & \dots & & & & & & 0 \\ 0 & 0 & \dots & 0 & 1 & \lambda & \dots & \lambda^{t_2-1} & 0 & \dots & & 0 \\ \vdots & & & & & & & & \ddots & & & \\ 0 & \dots & & & & & & & 0 & 1 & \dots & \lambda^{t_k-1} \end{pmatrix} \in \mathbb{F}_{q^m}^{k\times(t_1+\dots+t_k)}$$

$$\mathscr{C}_{\lambda,t_1,\dots,t_k} = \mathscr{C}_{\lambda,t_1} \oplus \cdots \oplus \mathscr{C}_{\lambda,t_k}$$

Completely decomposable codes

PS: Completely decomposable rank-metric codes

Completely decomposable codes of type $(n_1, \ldots, n_k)$

$$\mathscr{C} \sim \mathscr{C}_1 \oplus \cdots \oplus \mathscr{C}_k \qquad \mathscr{C}_i \to [n_i, 1]_{q^m/q} - \text{code}$$

Completely decomposable codes of type $(n_1, \dots, n_k)$

$$\mathscr{C} \sim \mathscr{C}_1 \oplus \cdots \oplus \mathscr{C}_k \qquad \mathscr{C}_i \to [n_i, 1]_{q^m/q} - \text{code}$$

This is equivalent to

- $\mathscr{C}$ admits a basis $\mathbf{c}_1, \dots, \mathbf{c}_k$, $n = \sum_{i=1}^{k} n_i$ and $n_i = w(\mathbf{c}_i)$
- $G = \begin{pmatrix} \mathbf{u}_1 & 0 & 0 & \cdots & 0 \\ 0 & \mathbf{u}_2 & 0 & \cdots & 0 \\ 0 & 0 & \ddots & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \cdots & \mathbf{u}_k \end{pmatrix}$ generator matrix of an equivalent code to $\mathscr{C}$

Completely decomposable codes of type $(n_1, \ldots, n_k)$

$$\mathscr{C} \sim \mathscr{C}_1 \oplus \cdots \oplus \mathscr{C}_k \quad \mathscr{C}_i \to [n_i, 1]_{q^m/q} - \text{code}$$

This is equivalent to

- $\mathscr{C}$ admits a basis $\mathbf{c}_1, \ldots, \mathbf{c}_k$, $n = \sum_{i=1}^{k} n_i$ and $n_i = w(\mathbf{c}_i)$
- $\mathscr{C}$ admits a basis $\mathbf{c}_1, \ldots, \mathbf{c}_k$, $\mathrm{supp}(\mathscr{C}) = \mathbb{F}_q^n$ and $\mathrm{supp}(\mathscr{C}) = \oplus_{i=1}^{k} \mathrm{supp}(\mathbf{c}_i)$

PS: Completely decomposable rank-metric codes

Completely decomposable codes of type $(n_1, \ldots, n_k)$

$$\mathscr{C} \sim \mathscr{C}_1 \oplus \cdots \oplus \mathscr{C}_k \quad \mathscr{C}_i \rightarrow [n_i, 1]_{q^m/q} - \text{code}$$

- More bounds on the weight distribution
- Study of new families of rank-metric codes

This is equivalent to

- $\mathscr{C}$ admits a basis $\mathbf{c}_1, \ldots, \mathbf{c}_k$, $n = \sum_{i=1}^{k} n_i$ and $n_i = w($
- $\mathscr{C}$ admits a basis $\mathbf{c}_1, \ldots, \mathbf{c}_k$, $\mathrm{supp}(\mathscr{C}) = \mathbb{F}_q^n$ and $\mathrm{supp}(\mathscr{C}) = \oplus_{i=1}^{k} \mathrm{supp}(\mathbf{c}_i)$

Thank you for your attention!