The geometric counterpart of maximum rank distance codes

Ferdinando Zullo
Università degli Studi della Campania "Luigi Vanvitelli"

Combinatorial Designs and Codes
12-16 July 2021

B. Csajbók, G. Marino, O. Polverino and FZ:
Maximum scattered linear sets and MRD-codes,
Journal of Algebraic Combinatorics (2017)

B. Csajbók, G. Marino, O. Polverino and FZ:
Generalising the scattered property of subspaces,
Combinatorica (2021)

V. Napolitano and FZ:
Codes with few weights arising from linear sets,
Advances in Mathematics of Communications (2020)

G. Zini and FZ:
Scattered subspaces and related codes,
Designs, Codes and Cryptography (2021)

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

Hamming distance

$$d(\mathbf{a}, \mathbf{b}) = |\{i : a_i \neq b_i, 1 \leq i \leq n\}|$$

Code: $\mathscr{C} \subseteq \mathbb{F}_q^n$

Singleton bound: $|\mathscr{C}| \leq q^{n-d+1}$,

$= \rightarrow$ MDS-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 projective systems

$\mathscr{C} \subseteq \mathbb{F}_q^n$

S. Ball:
On sets of vectors of a finite vector space in which every subset of basis size is a basis,
J. Eur. Math. Soc. 14 (2012)

J. I. Kokkala and P. R. J. Östergård:
Further results on the classification of MDS codes,
Adv. Math. Commun. 10 (2016)

S. Ball and M. Lavrauw:
Arcs in finite projective spaces,
EMS Surv. Math. Sci. 6 (2019)

$$n - d(\mathscr{C}) = \max\{|\mathcal{S} \cap H| : H \subset \mathrm{PG}(k-1,q), \dim(H) = k-2\}$$

$\mathscr{C}$ is MDS $\Leftrightarrow$ $\mathcal{S}$ is an n-arc

MDS conjecture
If $k < q$ then $m_q(k) = q+1$ except if q is even and $k \in \{2, q-2\}$

Rank metric codes

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

Rank distance

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

Code: $\mathscr{C} \subseteq \mathbb{F}_q^{n\times m}$

Singleton bound:

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

$= \rightarrow$ MRD-code

Minimum distance:

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

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

Rank distance

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

$$\mathrm{Hom}_{\mathbb{F}_q}(\mathbb{F}_q^m, \mathbb{F}_q^n)$$

Rank distance

$d(f,g) = \dim_{\mathbb{F}_q}(\mathrm{Im}(f-g))$

$$\mathscr{L}_{n,q} = \left\{ \sum_{i=0}^{n-1} a_i x^{q^i} \colon a_i \in \mathbb{F}_{q^n} \right\}$$

Rank distance

$d(f,g) = \dim_{\mathbb{F}_q}(\mathrm{Im}(f-g))$

Linear codes and q-projective systems

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

non-degenerate linear code

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

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

Randrianarisoa-2020

$U = \langle \mathbf{g}_1^t, \ldots, \mathbf{g}_n^t \rangle_{\mathbb{F}_q}$

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

$$n - d(\mathscr{C}) = \max\{w_{L_U}(H) : H \subset \mathrm{PG}(k-1,q), \dim(H) = k-2\}$$

$S = \mathrm{PG}(W, \mathbb{F}_{q^m}) \subseteq \mathrm{PG}(k-1, q^m)$

$w_{L_U}(S) = \dim_{\mathbb{F}_q}(U \cap W)$

$\mathscr{C}$ is MRD $\Leftrightarrow$ L_U is ???

k=2 and m=n Sheekey-2016

$\mathscr{C}$ is MRD $\Leftrightarrow$ $L_U \subseteq \mathrm{PG}(1,q^m)$ is such that $\dim_{\mathbb{F}_q}(U) = m$ and $w_{L_U}(P) \leq 1$

L_U is maximum scattered

n=km/2 Csajbók, Marino, Polverino and FZ-2017

$\mathscr{C}$ is MRD $\Leftrightarrow$ $L_U \subseteq \mathrm{PG}(k-1,q^m)$ is such that $\dim_{\mathbb{F}_q}(U) = \frac{km}{2}$ and $w_{L_U}(P) \leq 1$

L_U is maximum scattered

Blokhuis and Lavrauw-2000

If $L_U \subseteq \mathrm{PG}(k-1,q^m)$ is a scattered $\mathbb{F}_q$-linear set then $\mathrm{Rank}(L_U) \leq \frac{km}{2}$

k=2 and m=n Sheekey-2016

$\mathscr{C}$ is MRD $\Leftrightarrow$ $L_U \subseteq \mathrm{PG}(1,q^m)$ is such that $\dim_{\mathbb{F}_q}(U) = m$ and $w_{L_U}(P) \leq 1$

L_U is maximum scattered

n=km/2 Csajbók, Marino, Polverino and FZ-2017

$\mathscr{C}$ is MRD $\Leftrightarrow$ $L_U \subseteq \mathrm{PG}(k-1,q^m)$ is such that $\dim_{\mathbb{F}_q}(U) = \frac{km}{2}$ and $w_{L_U}(P) \leq 1$

L_U is maximum scattered

Blokhuis and Lavrauw-2000

L_U scattered $\mathrm{Rank}(L_U) \leq \frac{km}{2}$

- ✓ k even (Blokhuis and Lavrauw-2000)
- ✓ k=3 and m=4 (Ball, Blokhuis and Lavrauw-2000)
- ✓ Most of the cases (Bartoli, Giulietti, Marino and Polverino-2018)
- ✓ All the cases (Csajbók, Marino, Polverino and FZ-2017)

Lunardon-2017

m=n

Sheekey and Van de Voorde-2020

$\mathscr{C}$ is MRD $\Leftrightarrow$ $L_U \subseteq \mathrm{PG}(k-1,q^m)$ is such that $\dim_{\mathbb{F}_q}(U) = m$ and $w_{L_U}(H) \leq k-1$

L_U is scattered w.r.t. hyperplanes

n=km/(h+1) Zini and FZ-2021

$\mathscr{C}$ is MRD $\Leftrightarrow$ $L_U \subseteq \mathrm{PG}(k-1,q^m)$ is such that $\dim_{\mathbb{F}_q}(U) = \frac{km}{h+1}$ and $w_{L_U}(S) \leq h$ for all $S = \mathrm{PG}(h-1,q^m)$

L_U is scattered w.r.t. h-subspaces

Csajbók, Marino, Polverino and FZ-2021

If $L_U \subseteq \mathrm{PG}(k-1,q^m)$ is a h-scattered $\mathbb{F}_q$-linear set then $\mathrm{Rank}(L_U) \leq \frac{km}{h+1}$

m=n

Lunardon-2017

Sheekey and Van de Voorde-2020

$\mathscr{C}$ is MRD $\Leftrightarrow$ $L_U \subseteq \mathrm{PG}(k-1,q^m)$ is such that $\dim_{\mathbb{F}_q}(U) = m$ and $w_{L_U}(H) \leq k-1$

L_U is scattered w.r.t. hyperplanes

n=km/(h+1) Zini and FZ-2021

$\mathscr{C}$ is MRD $\Leftrightarrow$ $L_U \subseteq \mathrm{PG}(k-1,q^m)$ is such that $\dim_{\mathbb{F}_q}(U) = \frac{km}{h+1}$ and $w_{L_U}(S) \leq h$ for all $S = \mathrm{PG}(h-1,q^m)$

L_U is scattered w.r.t. h-subspaces

Csajbók, Marino, Polverino and FZ-2021

$\mathrm{Rank}(L_U) \leq \frac{km}{h+1}$

- ✓ h+1 divides k
- ✓ h=m-3 and k odd

Constructions of MRD codes

Generalized Gabidulin codes

$$\mathcal{G}_{m,k,s} = \langle x, x^{q^s}, \ldots, x^{q^{s(k-1)}} \rangle_{\mathbb{F}_{q^m}}$$

$k \leq m$
$\gcd(s, m) = 1$

Generalized twisted Gabidulin codes

$$\mathcal{H}_{m,k,s}(\delta, h) = \{a_0 x + a_1 x^{q^s} + \ldots + a_{k-1} x^{q^{s(k-1)}} + \delta a_0^{q^h} x^{q^{sk}} : a_i \in \mathbb{F}_{q^m}\}$$

$k \leq m$
$\gcd(s, m) = 1$
$\mathrm{N}_{q^m/q}(\delta) \neq (-1)^{mk}$

J. Sheekey:
A new family of linear maximum rank distance codes,
Adv. Math. Commun. 10(3) (2016)

- K. Otal and F. Ozbudak: Additive rank-metric codes, IEEE Trans. Inform. Theory 63 (2017)
- R. Trombetti and Y. Zhou: A new family of MRD codes in $\mathbb{F}_q^{2n\times 2n}$ with right and middle nuclei $\mathbb{F}_{q^n}$, IEEE Trans. Inform. Theory 65(2) (2018)
- J. Sheekey: New semifields and new MRD codes from skew polynomial rings, J. Lond. Math. Soc. 101(1) (2020)

Bartoli, Csajbók, Longobardi, Marino, Montanucci, Neri, Polverino, Santonastaso, Zanella, Zhou, FZ...

Constructions of MRD codes

Let $g: \mathbb{F}_{q^n} \to \mathbb{F}_{q^m}$ be an $\mathbb{F}_q$-linear map of rank $n \leq m$.
Let $\mathscr{C} \subseteq \mathscr{L}_{m,q}$ be an $\mathbb{F}_q$-linear RM-code.
The RM-code $g \circ \mathscr{C}$ is said the **punctured code** of $\mathscr{C}$.

Let L_U be an h-scattered $\mathbb{F}_q$-linear set of rank $\frac{km}{h+1}$ in

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

If $h+1 \nmid k$ then the associated code is not equivalent to a punctured code of neither a **generalized Gabidulin code** nor of **generalized twisted Gabidulin code**.

If $\mathscr{C}$ is a punctured code of $\mathscr{G}_{m,k,s}$ or $\mathscr{H}_{m,k,s}(\eta, h)$, then

$$|L(\mathscr{C})| = q^{\ell}, \text{ with } \ell \mid n$$

Few weight codes in Hamming metric

$L_U \subseteq \mathrm{PG}(k-1, q^m)$ is maximum h-scattered if

- $\dim_{\mathbb{F}_q}(U) = \dfrac{km}{h+1}$

$L_U \to$ projective system

$\mathscr{C}_{L_U}$ is a $[\theta_{km/(h+1)}, k]$-linear code having at most $h+1$ distinct weights

- Possible weights $\longrightarrow \theta_{km/(h+1)} - \theta_{km/(h+1)-m+i}$, $0 \le i \le h$
- Number of codewords of weight $\theta_{km/(h+1)} - \theta_{km/(h+1)-m+i} = \pi_{km/(h+1)-m+i}$

$$\frac{km}{h+1} - n \le w_{L_U}(\mathscr{H}) \le \frac{km}{h+1} - m + h$$

π_j = #hyperplanes of weight j

Few weight codes in Hamming metric

$L_U \rightarrow$ projective system

$\mathscr{C}_{L_U}$ is a $[\theta_{km/(h+1)}, k]$-linear code having at most $h+1$ distinct weights

* Possible weights $\longrightarrow \theta_{km/(h+1)} - \theta_{km/(h+1)-m+i}$, $0 \leq i \leq h$
* Number of codewords of weight $\theta_{km/(h+1)} - \theta_{km/(h+1)-m+i} = \pi_{km/(h+1)-m+i}$

$$\pi_{\frac{km}{h+1}-m+i} = A_{m-i}, \qquad i \in \{0, \ldots, h\}$$

Weight distribution of the rank metric code associated with L_U

MRD

Few weight codes in Hamming metric

$L_U \to$ projective system

$\mathscr{C}_{L_U}$ is a $[\theta_{km/(h+1),k}]$-linear code having at most $h+1$ distinct weights

- Po
- Nu

- A. Ravagnani: Rank-metric codes and their duality theory, Des. Codes Cryptogr. 80(1) (2016)
- G. Lunardon, R. Trombetti and Y. Zhou: On kernels and nuclei of rank metric codes, J. Algebraic Combin. 46 (2017)

$$\pi_{\frac{km}{h+1}-m+i} = A_{m-i}, \qquad i \in \{0,\dots,h\}$$

$$A_{d+\ell} = \begin{bmatrix} \frac{km}{h+1} \\ d+\ell \end{bmatrix}_q \sum_{t=0}^{\ell} (-1)^{t-\ell} \begin{bmatrix} \ell+d \\ \ell-t \end{bmatrix}_q q^{\binom{\ell-t}{2}} (q^{m(t+1)}-1) \quad > 0$$

Few weight codes in Hamming metric

$L_U \to$ projective system

$\mathscr{C}_{L_U}$ is a $[\theta_{km/(h+1)}, k]$-linear code having at most $h+1$ distinct weights

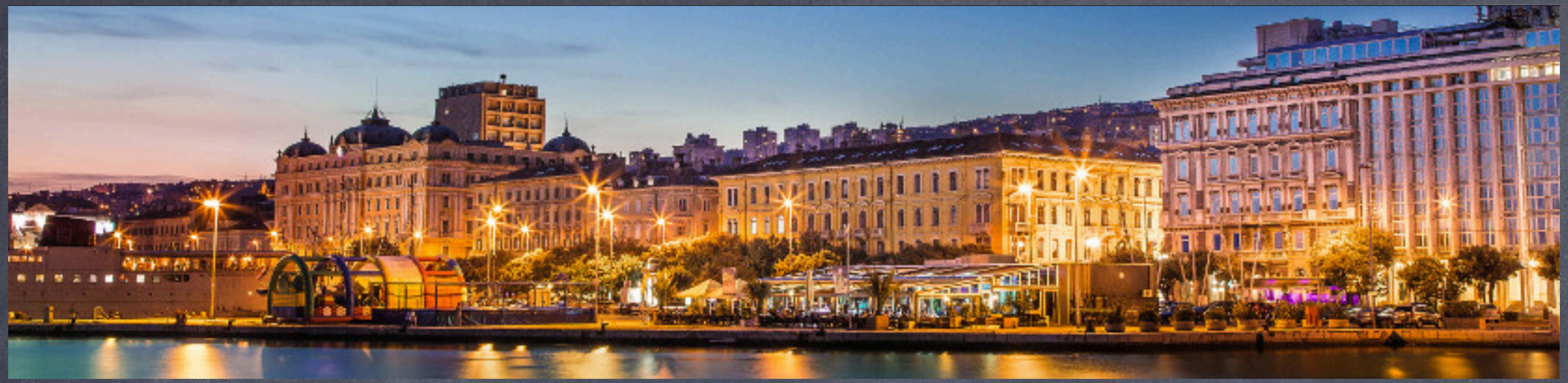
* Possible weights $\longrightarrow \theta_{km/(h+1)} - \theta_{km/(h+1)-m+i}$, $0 \le i \le h$
* Number of codewords of weight $\theta_{km/(h+1)} - \theta_{km/(h+1)-m+i} = \pi_{km/(h+1)-m+i}$

$$\pi_{\frac{km}{h+1}-m+i} = A_{m-i} > 0, \qquad i \in \{0, \dots, h\}$$

$(h+1)$-weight code

V. Napolitano and FZ:
Codes with few weights arising from linear sets,
Advances in Mathematics of Communications (2020)

G. Zini and FZ:
Scattered subspaces and related codes,
Designs, Codes and Cryptography (2021)



Thank you for your attention !