On 3-dimensional MRD codes

Francesco Ghiandoni

Joint work with D. Bartoli

OpeRA 2024, Open Problems on Rank-Metric Codes

Caserta, 14-16 Febbraio 2024

Rank metric codes

- $\mathbb{F}_q^{m\times n}$ $\mathbb{F}_q$-vector space
- Rank distance: $d(A,B) = \mathrm{rank}(A-B)$ for $A, B \in \mathbb{F}_q^{m\times n}$
- Code: $\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$
- $\mathbb{F}_q$-linear code: $\mathcal{C} \leq \mathbb{F}_q^{m\times n}$
- Minimum distance: $d = d(\mathcal{C}) = \min\{d(A,B) : A, B \in \mathcal{C}, A \neq B\}$
- Singleton bound: $|\mathcal{C}| \leq q^{\max\{m,n\}(\min\{m,n\}-d+1)}$
  - $= \rightarrow$ MRD code
- $\mathcal{C}, \mathcal{C}' \leq \mathbb{F}_q^{m\times n}$ equivalent: there exist $A \in \mathrm{GL}(m,q)$, $B \in \mathrm{GL}(n,q)$, and $\rho \in \mathrm{Aut}(\mathbb{F}_q)$ s.t.

$$\mathcal{C}' = A\mathcal{C}^\rho B = \{AC^\rho B : C \in \mathcal{C}\}$$

Linear rank metric codes as linearized polynomials

- $n = m$
- $\mathbb{F}_q^{n\times n} \simeq \mathcal{L}_{n,q} = \left\{ \sum_{i=0}^{n-1} a_i x^{q^i} : a_i \in \mathbb{F}_{q^n} \right\}$
- Rank distance: $\mathrm{d}(f,g) = \dim_{\mathbb{F}_q}(\mathrm{Im}(f-g))$
- $\mathcal{C}, \mathcal{C}' \leq \mathcal{L}_{n,q}$ equivalent: there exist two invertible $\mathbb{F}_q$-linearized polynomials $g(x), h(x) \in \mathcal{L}_{n,q}$ and $\rho \in \mathrm{Aut}(\mathbb{F}_q)$ s.t.

$$\mathcal{C}' = g \circ \mathcal{C}^\rho \circ h = \{g \circ f^\rho \circ h : \ f \in \mathcal{C}\}$$

- Left idealizer of $\mathcal{C}$: $L(\mathcal{C}) = \{\varphi(x) \in \mathcal{L}_{n,q} : \varphi \circ f \in \mathcal{C} \ \text{ for all } f \in \mathcal{C}\}$
- $\mathcal{C}$ $\mathbb{F}_{q^n}$-linear code: $L(\mathcal{C})$ contains a subring $\simeq \mathbb{F}_{q^n}$

Exceptional $\mathbb{F}_{q^n}$-linear MRD codes

Definition

An $\mathbb{F}_{q^n}$-linear code $\mathcal{C} \leq \mathcal{L}_{n,q}$ with minimum distance d is maximum rank distance (MRD) if $\dim_{\mathbb{F}_{q^n}}(\mathcal{C}) = n - d + 1$.
An $\mathbb{F}_{q^n}$-linear MRD code is an exceptional MRD code if

$$\mathcal{C}_\ell = \langle \mathcal{C} \rangle_{\mathbb{F}_{q^{n\ell}}} \leq \mathcal{L}_{n\ell,q}$$

is an MRD code for infinitely many ℓ

[Bartoli, Zini, Zullo. *IEEE Tran. Inf. Theory*, 2023]

- Up to equivalence, only two families of exceptional $\mathbb{F}_{q^n}$-linear MRD codes are known
  - (G) $\mathcal{G}_{r,s} = \langle x, x^{q^s}, \ldots, x^{q^{s(r-1)}} \rangle_{\mathbb{F}_{q^n}}$, with $\gcd(s,n) = 1$,;
  - (T) $\mathcal{H}_{r,s}(\delta) = \langle x^{q^s}, \ldots, x^{q^{s(r-1)}}, x + \delta x^{q^{sr}} \rangle_{\mathbb{F}_{q^n}}$, with $\gcd(s,n) = 1$ and $N_{q^n/q}(\delta) \neq (-1)^{nr}$

Exceptional $\mathbb{F}_{q^n}$-linear MRD codes

Definition

An $\mathbb{F}_{q^n}$-linear code $\mathcal{C} \leq \mathcal{L}_{n,q}$ with minimum distance d is maximum rank distance (MRD) if $\dim_{\mathbb{F}_{q^n}}(\mathcal{C}) = n - d + 1$.
An $\mathbb{F}_{q^n}$-linear MRD code is an exceptional MRD code if

$$\mathcal{C}_\ell = \langle \mathcal{C} \rangle_{\mathbb{F}_{q^{n\ell}}} \leq \mathcal{L}_{n\ell,q}$$

is an MRD code for infinitely many ℓ

[Bartoli, Zini, Zullo. *IEEE Tran. Inf. Theory*, 2023]

- Up to equivalence, only two families of exceptional $\mathbb{F}_{q^n}$-linear MRD codes are known
  - (G) $\mathcal{G}_{r,s} = \langle x, x^{q^s}, \ldots, x^{q^{s(r-1)}} \rangle_{\mathbb{F}_{q^n}}$, with $\gcd(s,n) = 1$,;
  - (T) $\mathcal{H}_{r,s}(\delta) = \langle x^{q^s}, \ldots, x^{q^{s(r-1)}}, x + \delta x^{q^{sr}} \rangle_{\mathbb{F}_{q^n}}$, with $\gcd(s,n) = 1$ and $N_{q^n/q}(\delta) \neq (-1)^{nr}$

MRD codes and scattered polynomials

- $f(X) = \sum A_i X^{q^i} \in \mathbb{F}_{q^n}[X]$ a q-polynomial;

Proposition

$$\mathcal{C}_f = \langle x, f(x) \rangle_{\mathbb{F}_{q^n}} \text{ 2-dimensional MRD code}$$

$$\Updownarrow$$

$$\frac{f(x)}{x} = \frac{f(y)}{y} \iff \frac{y}{x} \in \mathbb{F}_q, \quad \text{for } x, y \in \mathbb{F}_{q^n} \setminus \{0\}. \tag{1}$$

- A q-polynomial satisfying (1) is called a **scattered polynomial**

Non-monomial scattered polynomials for arbitrary n

- Almost all constructions of scattered polynomials for arbitrary n can be summarized as one family

$$f(X) = \delta X^{q^s} + X^{q^{n-s}} \tag{2}$$

where $\gcd(s, n) = 1$ and $\mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\delta) = \delta^{(q^n-1)/(q-1)} \neq 1$.

- Taking $t = s$, from (2) it follows that

$$\mathcal{C}_s = \langle x^{q^s}, x + \delta x^{q^{2s}} \rangle_{\mathbb{F}_{q^{mn}}}$$

is a 2-dimensional MRD code for all m satisfying $\gcd(mn, s) = 1$.

Non-monomial scattered polynomials for arbitrary n

- Almost all constructions of scattered polynomials for arbitrary n can be summarized as one family

$$f(X) = \delta X^{q^s} + X^{q^{n-s}} \qquad (2)$$

where $\gcd(s, n) = 1$ and $\mathrm{Norm}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\delta) = \delta^{(q^n-1)/(q-1)} \neq 1$.

- Taking $t = s$, from (2) it follows that

$$\mathcal{C}_s = \langle x^{q^s}, x + \delta x^{q^{2s}} \rangle_{\mathbb{F}_{q^{mn}}}$$

is a 2-dimensional MRD code for all m satisfying $\gcd(mn, s) = 1$.

Exceptional scattered polynomials of index t

- $0 \leq t \leq n-1$, $f \in \mathbb{F}_{q^n}[X]$ a q-polynomial

Definition

$\mathcal{C}_{f,t} = \langle x^{q^t}, f(x) \rangle_{\mathbb{F}_{q^n}}$ 2-dimensional MRD code $\iff$ $f(x)$ scattered of index t

$\mathcal{C}_{f,t} = \langle x^{q^t}, f(x) \rangle_{\mathbb{F}_{q^n}}$ *2-dimensional exceptional MRD code* $\iff$ $f(x)$ *exceptional scattered of index* t

[Sheekey. *Adv. Math. Commun.*, 2016] [Bartoli, Zhou. *J. Algebra*, 2018]

Scattered polynomials and algebraic curves

Proposition

$$\mathcal{C}_{f,t} = \langle x^{q^t}, f(x)\rangle_{\mathbb{F}_{q^n}} \text{ 2-dimensional MRD code}$$

$$\Updownarrow$$

$$f(x) \text{ scattered of index } t$$

$$\Updownarrow$$

$$\mathcal{C}_f : \frac{f(X)Y^{q^t} - f(Y)X^{q^t}}{X^qY - XY^q} = 0 \text{ has only points } (x,y) \text{ in } \mathbb{F}_{q^n}^2 \text{ with } \frac{y}{x} \in \mathbb{F}_q$$

- Know examples of exceptional scattered polynomials:
  - (Ps) $f(x) = x^{q^t}$ of index 0, with $\gcd(t,n) = 1$;
  - (LP) $f(x) = x + \delta x^{q^{2t}}$ of index t, with $\gcd(t,n) = 1$ and $N_{q^n/q}(\delta) = \delta^{(q^n-1)/(q-1)} \neq 1$.

Scattered polynomials and algebraic curves

Proposition

$$\mathcal{C}_{f,t} = \langle x^{q^t}, f(x)\rangle_{\mathbb{F}_{q^n}} \text{ 2-dimensional MRD code}$$

$$\Updownarrow$$

$$f(x) \text{ scattered of index } t$$

$$\Updownarrow$$

$$\mathcal{C}_f : \frac{f(X)Y^{q^t} - f(Y)X^{q^t}}{X^qY - XY^q} = 0 \text{ has only points } (x, y) \text{ in } \mathbb{F}_{q^n}^2 \text{ with } \frac{y}{x} \in \mathbb{F}_q$$

- Know examples of exceptional scattered polynomials:
  - (Ps) $f(x) = x^{q^t}$ of index 0, with $\gcd(t, n) = 1$;
  - (LP) $f(x) = x + \delta x^{q^{2t}}$ of index t, with $\gcd(t, n) = 1$ and $N_{q^n/q}(\delta) = \delta^{(q^n-1)/(q-1)} \neq 1$.

Non-existence results for 2-dim exceptional MRD codes

- index $0, 1$

Theorem (Bartoli, Zhou, 2018)

- *X^{q^k} is the unique exceptional scattered monic polynomial of index 0*
- *The only exceptional scattered monic polynomials of index 1 over $\mathbb{F}_{q^n}$ are X and $bX + X^{q^2}$, where $N_{q^n/q}(b) \neq 1$*

- index $t > 1$

Theorem (Bartoli,Montanucci, 2020)

Let $f(X) = \sum_{i=0}^{M} A_i X^{q^{k_i}} \in \mathbb{F}_{q^n}[X]$, where $A_M = 1$, $k_0 = 0$, and either

- *$k_1 = 1$, $k_i \geq t$ for $i \geq 2$ and $k_M \geq t + 2$, or*
- *$k_1 > t$.*

If either $k_M \geq 3t$ and $t \mid k_M$, or $k_M \geq 2t - 1$ and $t \nmid k_M$, then $f(X)$ is not an exceptional scattered polynomial of index t

Scattered subspaces

Definition

Let $h, r, n \in \mathbb{N}$ $\quad h < r$, and $U \subseteq V(r, q^n)$ an $\mathbb{F}_q$-subspace.

$$U \text{ } h\text{-scattered in } V(r,q^n) \iff \begin{array}{c} \dim_{\mathbb{F}_q}(U \cap H) \leq h \\ \forall\ H \subseteq V(r,q^n),\ \dim_{\mathbb{F}_{q^n}}(H) = h. \end{array}$$

[Csajbók, Marino, Polverino, Zullo. *Combinatorica*, 2021]

Theorem (Csajbók, Marino, Polverino, Zullo, 2021)

$$\begin{array}{c} U \ h\text{-scattered in } V(r,q^n) \\ U \text{ not a subgeometry} \end{array} \implies \dim_{\mathbb{F}_q}(U) \leq \frac{rn}{h+1}.$$

- If $\dim_{\mathbb{F}_q}(U) = \frac{rn}{h+1}$, U is said maximum h-scattered in $V(r, q^n)$.

Scattered sequences

Definition

Let $\mathcal{I} := (i_1, i_2, \ldots, i_m) \in (\mathbb{Z}/n\mathbb{Z})^m$ and $f_1, \ldots, f_s \in \mathcal{L}_{n,q}[X_1, \ldots, X_m]$.

$\underline{f} := (f_1, \ldots, f_s)$ $(\mathcal{I}; h)_{q^n}$-scattered sequence of order m

$$\Updownarrow$$

$$\mathcal{U}_{\mathcal{I},\underline{f}} := \{(x_1^{q^{i_1}}, \ldots, x_m^{q^{i_m}}, f_1(x_1, \ldots, x_m), \ldots, f_s(x_1, \ldots, x_m)) : x_j \in \mathbb{F}_{q^n}\}$$

maximum h-scattered in $V(m+s, q^n)$.

$\underline{f} := (f_1, \ldots, f_s)$ *exceptional* $(\mathcal{I}; h)_{q^n}$*-scattered sequence of order* m

$$\Updownarrow$$

$\mathcal{U}_{\mathcal{I},\underline{f}}$ *maximum* h*-scattered in* $V(m+s, q^{\ell n})$, *for infinitely many* ℓ

[Bartoli, Marino, Neri, Vicino. *arXiv:2211.11477*, 2022]

$m = 1 \ldots$ Moore polynomial sets

- Let $m = 1$, $\mathcal{I} = \{t\}$, and $f_2, \ldots, f_r$ in $\mathcal{L}_{n,q}[X]$.

Proposition

$$(f_2, \ldots, f_r) \quad (\mathcal{I}; r-1)_{q^n}\text{-scattered sequence of order } 1$$

$$\Updownarrow$$

$$\forall\, \alpha_1, \ldots, \alpha_r \in \mathbb{F}_{q^n}:$$

$$\det \begin{pmatrix} \alpha_1^{q^t} & f_2(\alpha_1) & \cdots & f_r(\alpha_1) \\ \alpha_2^{q^t} & f_2(\alpha_2) & \cdots & f_r(\alpha_2) \\ \vdots & \vdots & \cdots & \vdots \\ \alpha_r^{q^t} & f_2(\alpha_r) & \cdots & f_r(\alpha_r) \end{pmatrix} = 0 \quad \Longrightarrow \quad \dim_{\mathbb{F}_q} \langle \alpha_1, \ldots, \alpha_r \rangle_{\mathbb{F}_q} < r;$$

- $\underline{f} = (x^{q^t}, f_2, \ldots, f_r)$ is said to be a **Moore polynomial set** for q and n

Bartoli, Zini and Zullo *Linear Maximum Rank Distance Codes of Exceptional Type*, IEEE Tran. Inf. Theory, 69(6):3627–3636, 2023.

Link with MRD codes

Theorem (Bartoli, Zini, Zullo, 2023)

Let $r \leq n+1$ *and* $x^{q^t}, f_2(x), \ldots, f_r(x) \in \mathcal{L}_{n,q}$ $\mathbb{F}_{q^n}$*-linearly independent.*

$\underline{f} = (x^{q^t}, f_2(x), \ldots, f_r(x))$ *Moore polynomial set for q and n*	$\Longleftrightarrow$	$\mathcal{C}_{\underline{f}} = \langle x^{q^t}, f_2(x), \ldots, f_r(x) \rangle_{\mathbb{F}_{q^n}}$ $\mathbb{F}_{q^n}$*-linear MRD code of dimension r*

Assumptions on $f_1, \dots, f_r$

- Consider codes $\mathcal{C}$ containing a monomial.

Proposition (Bartoli,Zini,Zullo, 2023)

Given a non-degenerate $\mathbb{F}_{q^n}$-linear code $\mathcal{C}$ of dimension r, there exist $f_1(x), \dots, f_r(x) \in \mathcal{C}$ such that the following properties hold:

(1) $f_1(x) = x^{q^t}$;

(2) $f_1(x), \dots, f_r(x)$ *are $\mathbb{F}_{q^n}$-linearly independent;*

(3) $M_1 := \deg_q(f_1(x)), \dots, M_r := \deg_q(f_r(x))$ *are all distinct;*

(4) $m_1 := \min \deg_q(f_1(x)), \dots, m_r := \min \deg_q(f_r(x))$ *are all distinct, and $m_i = 0$ for some i;*

(5) $f_1(x), \dots, f_r(x)$ *are monic;*

(6) *for any i, if $f_i(x)$ is a monomial then $m_i = M_i \geq t$.*

- t is said to be the index of $\mathcal{C}$

Exceptionality results...$t = 0$

Theorem (Bartoli,Zini,Zullo, 2023)

- $\mathcal{C} = \langle x, g_2(x), g_3(x), \ldots, g_r(x) \rangle_{\mathbb{F}_{q^n}}$ *exceptional MRD of index* 0
- $\deg_q(g_r(x)) > \deg_q(g_{r-1}(x)) > \cdots > \deg_q(g_2(x))$
- $(q, \deg_q(g_2(x))) \notin \{(2,2),(2,4),(3,2),(4,2),(5,2)\}$

$$\Downarrow$$

$\mathcal{C}$ is a generalized Gabidulin code

Exceptionality results...$t > 0$

- $t > 0$ and $r \geq 3$
- $f(x), g_3(x), \ldots, g_r(x)$ in $\mathcal{L}_{n,q}$
- $f(x)$ separable

Theorem (Bartoli,Zini,Zullo,2023)

$\mathcal{C} = \langle x^{q^t}, f(x), g_3(x), \ldots, g_r(x)\rangle_{\mathbb{F}_{q^n}}$
exceptional MRD of index t
$\deg(g_i(x)) > \max\{q^t, \deg(f(x))\}$
$\forall\ i = 3, \ldots, r$

$\Longrightarrow$

$f(x)$ *exceptional scattered of index t*

$\langle x^{q^t}, f(x)\rangle_{\mathbb{F}_{q^n}}$
exceptional 2-dim MRD code

$\subseteq$

$\langle x^{q^t}, f(x), g_3(x), \ldots, g_r(x)\rangle_{\mathbb{F}_{q^n}}$
exceptional r-dim MRD code

Open problem

Conjecture

If $\min\{\deg(g_i(x)) : i = 3, \ldots, r\} > \max\{q^t, \deg(f(x))\}$, *there are no exceptional* $\mathbb{F}_{q^n}$*-linear MRD codes of index* t *of type*

$$\mathcal{C} = \langle x^{q^t}, f(x), g_3(x), \ldots, g_r(x)\rangle_{\mathbb{F}_{q^n}}$$

[Bartoli, Zini, Zullo. *IEEE Tran. Inf. Theory*, 2023]

- Partial answer:
  - $r = 3$
  - $f(x)$ a LP polynomial, i.e

$$f(x) = x + \delta x^{q^{2t}}$$

$$\gcd(t, n) = 1 \text{ and } N_{q^n/q}(\delta) = \delta^{(q^n-1)/(q-1)} \neq 1$$

Open problem

Conjecture

If $\min\{\deg(g_i(x)) : i = 3, \ldots, r\} > \max\{q^t, \deg(f(x))\}$, *there are no exceptional* $\mathbb{F}_{q^n}$*-linear MRD codes of index* t *of type*

$$\mathcal{C} = \langle x^{q^t}, f(x), g_3(x), \ldots, g_r(x) \rangle_{\mathbb{F}_{q^n}}$$

[Bartoli, Zini, Zullo. *IEEE Tran. Inf. Theory*, 2023]

- Partial answer:
  - $r = 3$
  - $f(x)$ a LP polynomial, i.e

$$f(x) = x + \delta x^{q^{2t}}$$

$$\gcd(t, n) = 1 \text{ and } N_{q^n/q}(\delta) = \delta^{(q^n-1)/(q-1)} \neq 1$$

Proposition (Bartoli,Zini,Zullo, 2023)

$\underline{f} = (x^{q^t}, f(x), g(x))$ Moore polynomial set for q and n of index t

$$\iff \mathcal{A}_{\underline{f}} : \frac{\begin{vmatrix} X^{q^t} & f(X) & g(X) \\ Y^{q^t} & f(Y) & g(Y) \\ Z^{q^t} & f(Z) & g(Z) \end{vmatrix}}{\begin{vmatrix} X & X^q & X^{q^2} \\ Y & Y^q & Y^{q^2} \\ Z & Z^q & Z^{q^2} \end{vmatrix}} = 0$$

has only points $(x : y : z) \in PG(2, q^n)$ with $\alpha x + \beta y + \gamma z = 0$ for suitable $\alpha, \beta, \gamma \in \mathbb{F}_q$

Corollary

If $\mathcal{A}_{\underline{f}}$ has a $\mathbb{F}_{q^n}$-rational absolutely irreducible component, then $\mathcal{C}_{\underline{f}} = \langle x^{q^t}, f(x), g(x) \rangle_{\mathbb{F}_{q^n}}$ is not an exceptional MRD code

3-dimensional codes of type $\langle x^{q^t}, x+\delta x^{q^{2t}}, g(x)\rangle_{\mathbb{F}_{q^n}}$

Proposition

If $(x+\delta x^{q^{2t}}, G(x)) \subseteq \mathcal{L}_{n,q}$ is a $(\{t\},2)_{q^n}$-scattered sequence of order 1 and $n > 4\deg_q(G)+2$, then $\min\deg_q(G) = 2t$ or $\min\deg_q(G) = t/2$.

- Investigation of $\mathbb{F}_{q^n}$-rational absolutely irreducible components of the surface in $\mathrm{PG}(3,q^n)$ with affine equation

$$\begin{vmatrix} X^{q^t} & X+\delta X^{q^{2t}} & X^{q^{2t}}+\cdots+CX^{q^k} \\ Y^{q^t} & Y+\delta Y^{q^{2t}} & Y^{q^{2t}}+\cdots+CY^{q^k} \\ Z^{q^t} & Z+\delta Z^{q^{2t}} & Z^{q^{2t}}+\cdots+CZ^{q^k} \end{vmatrix} = 0$$

or

$$\begin{vmatrix} X^{q^t} & X+\delta X^{q^{t2t}} & X^{q^{t/2}}+\cdots+CX^{q^k} \\ Y^{q^t} & Y+\delta Y^{q^{2t}} & Y^{q^{t/2}}+\cdots+CY^{q^k} \\ Z^{q^t} & Z+\delta Z^{q^{2t}} & Z^{q^{t/2}}+\cdots+CZ^{q^k} \end{vmatrix} = 0$$

New results

Theorem (Bartoli, G., 2024)

Let $\underline{f} = (x^{q^t}, x + \delta x^{q^{2t}}, g(x))$, *where* $\delta^{(q^n-1)/(q-1)} \neq 1$, $\deg_q(g) > 2t$ *and* $\mathrm{mindeg}_q(g) = 2t$ *or* $t/2$.
Then $\mathcal{A}_{\underline{f}}$ *has an absolutely irreducible component defined over* $\mathbb{F}_{q^n}$ *and not contained in*

$$\begin{vmatrix} X & X^q & X^{q^2} \\ Y & Y^q & Y^{q^2} \\ Z & Z^q & Z^{q^2} \end{vmatrix} = 0$$

Theorem (Bartoli, G., 2024)

Let $\underline{f} = (x^{q^t}, x + \delta x^{q^{2t}}, g(x))$, *where* $\delta^{(q^n-1)/(q-1)} \neq 1$, $\deg_q(g) > 2t$ *and* $\mathrm{mindeg}_q(g) = 2t$ *or* $t/2$. *Then* $\mathcal{C}_{\underline{f}}$ *is not an exceptional MRD code*

$r \geq 3$ and $\deg(G(x)) < 2t$?

Find/prove the non-existence of r-dimensional exceptional MRD codes of type $\langle x^{q^t}, f(x), g_3(x), \ldots, g_r(x)\rangle_{\mathbb{F}_{q^n}}$ in the following cases:

- $r > 3$, $f(x) = x + \delta x^{q^{2t}}$ and $\deg(g_i(x)) > 2t$ for all $i = 3, \ldots, r$,
- $r = 3$ and $\max\{\deg(f(x)), \deg(g(x))\} < t$
- $r = 3$ and $\deg(f(x)) > \deg(g(x))$ inequivalent to (T)

THANK YOU FOR YOUR ATTENTION!