Recent results on scattered spaces and MRD codes

Daniele Bartoli

University of Perugia, Italy

OpeRA 2024

"Open Problems on Rank-Metric Codes"

Caserta, 14 - 16 February 2024

Outline

1. Linear sets, Scattered linear sets, and connections

Outline

1. Linear sets, Scattered linear sets, and connections

2. Maximum scattered linear sets in $\mathrm{PG}(1, \mathbb{F}_{q^n})$

Outline

1. Linear sets, Scattered linear sets, and connections
2. Maximum scattered linear sets in $\mathrm{PG}(1, \mathbb{F}_{q^n})$
3. Maximum r-scattered linear sets in $\mathrm{PG}(r, \mathbb{F}_{q^n})$

Outline

1. Linear sets, Scattered linear sets, and connections
2. Maximum scattered linear sets in $\mathrm{PG}(1, \mathbb{F}_{q^n})$
3. Maximum r-scattered linear sets in $\mathrm{PG}(r, \mathbb{F}_{q^n})$
4. Rank-metric codes

Outline

1. Linear sets, Scattered linear sets, and connections
2. Maximum scattered linear sets in $\mathrm{PG}(1, \mathbb{F}_{q^n})$
3. Maximum r-scattered linear sets in $\mathrm{PG}(r, \mathbb{F}_{q^n})$
4. Rank-metric codes
5. Scattered sequences

Linear sets and scattered linear sets

Definition (Linear sets)

$\mathbb{U} \leq_q \; \mathbb{F}_{q^n}^{r+1}$, $\dim_q(\mathbb{U}) = k$

$$L(\mathbb{U}) = \{\langle u\rangle_{\mathbb{F}_{q^n}} \; : \; u \in \mathbb{U} \setminus \{\mathbf{0}\}\} \subset \mathrm{PG}(r, \mathbb{F}_{q^n})$$

$\mathbb{F}_q$-linear set of $\mathrm{PG}(r, \mathbb{F}_{q^n})$ of rank k

$$|L(\mathbb{U})| \leq \frac{q^k - 1}{q - 1}$$

$$k \leq \frac{n(r+1)}{2}$$

[Blokhuis and Lavrauw 2000]

Definition (Maximum scattered Linear sets in $\mathrm{PG}(r, q^n)$)

$$\dim_q(\mathbb{U}) = k \leftarrow \text{maximum possible}$$

$$|L(\mathbb{U})| = \frac{q^k-1}{q-1} \leftarrow \text{maximum possible}$$

Some applications

- *blocking sets*

  Ball,Blokhuis,Lavrauw, Lunardon, Polverino, Trombetti, Zhou...
- *two-intersection sets*

  Blokhuis, Lavrauw...
- *finite semifields*

  Cardinali, Polverino, Trombetti, Ebert, Marino, Lunardon...
- *translation caps*

  B., Giulietti, Marino, Polverino...
- *translation hyperovals*

  Durante, Trombetti, Zhou...

1. Scattered and Maximum scattered linear sets are not rare in general

2. One seeks for sets with a prescribed shape in general

1. Scattered and Maximum scattered linear sets are not rare in general

2. One seeks for sets with a prescribed shape in general

"Geometric" constructions (projection, intersection, ...)

"polynomial" constructions (description via polynomials over finite fields)

Maximum Scattered linear sets in $\mathrm{PG}(1, q^n)$

$f(X) = \sum_i a_i X^{q^i} \in \mathbb{F}_{q^n}[X]$

$$\mathbb{U} = \{(x, f(x)) \ : \ x \in \mathbb{F}_{q^n}\} \leq \mathbb{F}_{q^n}^2$$

Definition (Maximum scattered Linear sets in $\mathrm{PG}(1, q^n)$)

$\dim_q(\mathbb{U}) = n$, $|L(\mathbb{U})| = \frac{q^n-1}{q-1}$ $\Longrightarrow$ $L(\mathbb{U})$ is Maximum scattered, $f(X)$ scattered polynomial (Sheekey 2016)

Scattered Polynomials

Definition (B.-ZHOU; J. Alg. 2018)

$f(X) = \sum_i a_i X^{q^i} \in \mathbb{F}_{q^n}[X]$ Scattered of index t if

$$\mathbb{U} = \left\{ (x^{q^t}, f(x)) \ : \ x \in \mathbb{F}_{q^n} \right\}$$

maximum scattered

Scattered Polynomials

Definition (B.-ZHOU; J. Alg. 2018)

$f(X) = \sum_i a_i X^{q^i} \in \mathbb{F}_{q^n}[X]$ Exceptional Scattered of index t if

$$\mathbb{U}_m = \left\{ (x^{q^t}, f(x)) \ : \ x \in \mathbb{F}_{q^{mn}} \right\}$$

maximum scattered for infinitely many m

Scattered Polynomials

Definition (B.-ZHOU; J. Alg. 2018)

$f(X) = \sum_i a_i X^{q^i} \in \mathbb{F}_{q^n}[X]$ Scattered of index t if

$$\mathbb{U} = \left\{(x^{q^t}, f(x)) \ : \ x \in \mathbb{F}_{q^n}\right\}$$

maximum scattered

Lemma

$$\mathbb{U} = \left\{(x^{q^t}, f(x)) \ : \ x \in \mathbb{F}_{q^n}\right\}$$

$L(\mathbb{U}) \subset \mathrm{PG}(1, q^n)$ *maximum scattered linear set* $\iff$

$$\mathcal{C}_f \ : \ \frac{f(X)Y^{q^t} - f(Y)X^{q^t}}{X^qY - XY^q} = 0 \subset \mathrm{PG}(2, q^n)$$

contains only points (x, y) *with* $\frac{y}{x} \in \mathbb{F}_q$

Scattered Polynomials

Lemma

$$\mathbb{U} = \left\{ (x^{q^t}, f(x)) \ : \ x \in \mathbb{F}_{q^n} \right\}$$

$L(\mathbb{U}) \subset \mathrm{PG}(1, q^n)$ *maximum scattered linear set* $\iff$

$$\mathcal{C}_f \ : \ \frac{f(X)Y^{q^t} - f(Y)X^{q^t}}{X^qY - XY^q} = 0 \subset \mathrm{PG}(2, q^n)$$

contains only points (x, y) *with* $\frac{y}{x} \in \mathbb{F}_q$

Hasse-Weil $\Longrightarrow \deg(\mathcal{C}_f) < q^{n/4}$

Scattered Polynomials

Lemma

$$\mathbb{U} = \left\{ (x^{q^t}, f(x)) \ : \ x \in \mathbb{F}_{q^n} \right\}$$

$L(\mathbb{U}) \subset \mathrm{PG}(1, q^n)$ *maximum scattered linear set* $\iff$

$$\mathcal{C}_f \ : \ \frac{f(X)Y^{q^t} - f(Y)X^{q^t}}{X^qY - XY^q} = 0 \subset \mathrm{PG}(2, q^n)$$

contains only points (x, y) *with* $\frac{y}{x} \in \mathbb{F}_q$

Hasse-Weil $\Longrightarrow \deg(\mathcal{C}_f) < q^{n/4}$

$\mathbb{U} = \{(x, f(x)) \ : \ x \in \mathbb{F}_{q^n}\} \Longrightarrow \mathbb{U} = \left\{ (x^{q^t}, g(x) = (f(x))^{q^t}) \ : \ x \in \mathbb{F}_{q^n} \right\}$

Scattered Polynomials

Lemma

$$\mathbb{U} = \left\{(x^{q^t}, f(x)) \;:\; x \in \mathbb{F}_{q^n}\right\}$$

$L(\mathbb{U}) \subset \mathrm{PG}(1, q^n)$ *maximum scattered linear set* $\iff$

$$\mathcal{C}_f \;:\; \frac{f(X)Y^{q^t} - f(Y)X^{q^t}}{X^qY - XY^q} = 0 \subset \mathrm{PG}(2, q^n)$$

contains only points (x, y) *with* $\frac{y}{x} \in \mathbb{F}_q$

Hasse-Weil $\Longrightarrow \deg(\mathcal{C}_f) < q^{n/4}$

$\mathbb{U} = \{(x, f(x)) \;:\; x \in \mathbb{F}_{q^n}\} \Longrightarrow \mathbb{U} = \left\{(x^{q^t}, g(x) = (f(x))^{q^t}) \;:\; x \in \mathbb{F}_{q^n}\right\}$

$$\deg\left(\frac{g(X)Y^{q^t} - g(Y)X^{q^t}}{X^qY - XY^q}\right) << \deg\left(\frac{f(X)Y - f(Y)X}{X^qY - XY^q}\right)$$

$$\mathcal{C}_f \;:\; \frac{f(X)Y^{q^t} - f(Y)X^{q^t}}{X^qY - XY^q} = 0$$

Theorem (B.-ZHOU; J. Alg. 2018)

- *INDEX* 0 $\Longrightarrow X^{q^k}$, $q > 5$
- *INDEX* 1 $\Longrightarrow$ X
  $bX + X^{q^2}$, $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(b) \neq 1$

$$\mathcal{C}_f \ : \ \frac{f(X)Y^{q^t} - f(Y)X^{q^t}}{X^qY - XY^q} = 0$$

Theorem (B.-ZHOU; J. Alg. 2018)

- *INDEX* 0 $\Longrightarrow X^{q^k}$, $q > 5$
- *INDEX* 1 $\Longrightarrow$ X
 $bX + X^{q^2}$, $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(b) \neq 1$

Tools

- *Estimation on the number and "type" of singular points*
- *Study the structure of the branches centered at singular points*

$$\mathcal{C}_f \quad : \quad \frac{f(X)Y^{q^t} - f(Y)X^{q^t}}{X^qY - XY^q} = 0$$

Theorem (B.-ZHOU; J. Alg. 2018)

- *INDEX* 0 $\Longrightarrow X^{q^k}$, $q > 5$
- *INDEX* 1 $\Longrightarrow$ X; $bX + X^{q^2}$, $N_{\mathbb{F}_{q^n}/\mathbb{F}_q}(b) \neq 1$

Tools

- *Estimation on the number and "type" of singular points*
- *Study the structure of the branches centered at singular points*

(B.-MONTANUCCI, JCTA 2021)

Classification of exceptional scattered monic polynomial of INDEX $t = 2$ and partial classification for INDEX $t > 2$

Exceptional Scattered polynomials via group theory

Theorem (Ferraguti, Micheli, J. Alg. 2021)

f linearized nonmonomial polynomial
$d := \max\{\deg_q(f), t\}$ odd prime $\Longrightarrow$ *f not exceptional scattered*

Exceptional Scattered polynomials via group theory

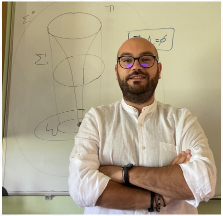
Theorem (Ferraguti, Micheli, J. Alg. 2021)

f linearized nonmonomial polynomial
$d := \max\{\deg_q(f), t\}$ *odd prime* $\Longrightarrow$ *f not exceptional scattered*


Theorem (B., Giulietti, Zini, 2022)

f linearized nonmonomial polynomial
$d := \max\{\deg_q(f), t\}$ *odd* $\Longrightarrow$ *f not exceptional scattered*

r-fat polynomials


Definition

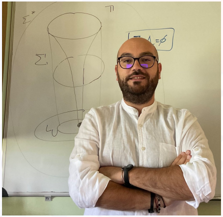
f linearized polynomial r-fat polynomial of index $t \in \{0, \dots, n-1\}$

$$\Updownarrow$$

$$\exists\ m_1, \dots, m_r \in \mathbb{F}_{q^n} :\ \dim_{\mathbb{F}_q} \ker(f(x) - m_i x^{q^t}) > 1$$

r-fat polynomials $\iff$ $U = \{(x^{q^t}, f(x)) : x \in \mathbb{F}_{q^n}\}$ *has r fat points*

r-fat polynomials

Theorem (B. Micheli, Zini, Zullo, JCTA 2021)

There exist no exceptional r-fat polynomials whenever $r > 0$

Maximum h-Scattered linear sets in $\mathrm{PG}(r, q^n)$

Definition (Linear sets)

$\mathbb{U} \leq_q \mathbb{F}_{q^n}^{r+1}$, $\dim_q(\mathbb{U}) = k$

$$L(\mathbb{U}) = \{\langle u\rangle_{\mathbb{F}_{q^n}} \ : \ u \in \mathbb{U} \setminus \{\mathbf{0}\}\} \subset \mathrm{PG}(r, \mathbb{F}_{q^n})$$

$\mathbb{F}_q$-linear set of $\mathrm{PG}(r, \mathbb{F}_{q^n})$ of rank k

Definition (Weight of a subspace)

$W \leq_{q^n} \mathbb{F}_{q^n}^{r+1}$

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

Definition (h-scattered subspace)

$\mathbb{U}$ is said *h-scattered* if

$$\forall W \subset \mathbb{F}_{q^n}^{r+1}, \dim_{\mathbb{F}_{q^n}}(W) = h \Longrightarrow w_{\mathbb{U}}(W) \leq h$$

Maximum h-Scattered linear sets in $\mathrm{PG}(r, q^n)$

Definition (Weight of a subspace)

$W \leq_{q^n} \mathbb{F}_{q^n}^{r+1}$

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

Definition (h-scattered subspace)

$\mathbb{U}$ is said *h-scattered* if

$$\forall W \subset \mathbb{F}_{q^n}^{r+1}, \dim_{\mathbb{F}_{q^n}}(W) = h \Longrightarrow w_{\mathbb{U}}(W) \leq h$$

1-scattered $\Longrightarrow$ scattered

$$k \leq \frac{n(r+1)}{h+1}$$

[Csajbók, Marino, Polverino, Zullo 2021]

Rank-metric codes

$$v = (v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n, \qquad u = (u_1, \ldots, u_n) \in \mathbb{F}_{q^m}^n$$

$$\mathrm{wt}_{\mathsf{rk}}(v) = \dim_{\mathbb{F}_q} \langle v_1, \ldots, v_n \rangle_{\mathbb{F}_q}$$ **rank weight** of v

$$\mathrm{d}_{\mathsf{rk}}(u, v) = \mathrm{wt}_{\mathsf{rk}}(u - v)$$ **rank distance**

Rank-metric codes

$$v = (v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n, \qquad u = (u_1, \ldots, u_n) \in \mathbb{F}_{q^m}^n$$

$$\mathrm{wt}_{\mathrm{rk}}(v) = \dim_{\mathbb{F}_q} \langle v_1, \ldots, v_n \rangle_{\mathbb{F}_q}$$ **rank weight** of v

$$\mathrm{d}_{\mathrm{rk}}(u, v) = \mathrm{wt}_{\mathrm{rk}}(u - v)$$ **rank distance**

Definition (Delsarte 1978 - Gabidulin 1985)

An $[n, k]_{q^m/q}$ **(rank-metric) code** is a k-dimensional $\mathbb{F}_{q^m}$-subspace of $\mathbb{F}_{q^m}^n$ endowed with the rank distance.

Rank-metric codes

$$d(\mathcal{C}) := d = \min\{\mathrm{wt}_{\mathrm{rk}}(v) : \ v \in \mathcal{C}, v \neq 0\}$$

$\mathcal{C}$ *is an* $[n, k, d]_{q^m/q}$ *code*

Theorem (Singleton Bound - Delsarte 1978)

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

$mk = \min\{m(n-d+1), n(m-d+1)\} \Rightarrow \mathcal{C}$ *Maximum Rank Distance*

Rank-metric codes

$$d(\mathcal{C}) := d = \min\{\mathrm{wt}_{\mathrm{rk}}(v) : \ v \in \mathcal{C}, v \neq 0\}$$

$\mathcal{C}$ *is an* $[n,k,d]_{q^m/q}$ *code*

Theorem (Singleton Bound - Delsarte 1978)

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

$mk = \min\{m(n-d+1), n(m-d+1)\} \Rightarrow \mathcal{C}$ *Maximum Rank Distance*

Theorem (Zini, Zullo 2021)

$n := \frac{km}{h+1}$ L_U *linear set of rank* n *in* $\mathrm{PG}(k-1, q^m)$

L_U *maximum h-scattered* $\iff$ $\mathcal{C}_U^{\perp}$ *MRD*

Rank-metric codes

$$d(\mathcal{C}) := d = \min\{\mathrm{wt}_{\mathrm{rk}}(v) : \ v \in \mathcal{C}, v \neq 0\}$$

$\mathcal{C}$ *is an* $[n,k,d]_{q^m/q}$ *code*

Theorem (Singleton Bound - Delsarte 1978)

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

$mk = \min\{m(n-d+1), n(m-d+1)\} \Rightarrow \mathcal{C}$ *Maximum Rank Distance*

Theorem (Zini, Zullo 2021)

$n := \frac{km}{h+1}$ $\qquad$ L_U *linear set of rank* n *in* $\mathrm{PG}(k-1, q^m)$

L_U *maximum h-scattered* $\iff$ $\mathcal{C}_U^{\perp}$ *MRD*

1. *Francesco's talk*
2. *Giuseppe's talk*

Maximum r-Scattered linear sets in $\mathrm{PG}(r, q^n)$

Consider the linear set

$$\mathbb{U} := \{(x^{q^t}, f_1(x), \ldots, f_r(x)) : x \in \mathbb{F}_{q^n}\}$$

where f_i are q-linearized

Maximum r-Scattered linear sets in $\mathrm{PG}(r, q^n)$

Consider the linear set

$$\mathbb{U} := \{(x^{q^t}, f_1(x), \ldots, f_r(x)) : x \in \mathbb{F}_{q^n}\}$$

where f_i are q-linearized

When $L(\mathbb{U})$ is maximum r-scattered?

Maximum r-Scattered linear sets in $\mathrm{PG}(r, q^n)$

Consider the linear set

$$\mathbb{U} := \{(x^{q^t}, f_1(x), \ldots, f_r(x)) : x \in \mathbb{F}_{q^n}\}$$

where f_i are q-linearized

When $L(\mathbb{U})$ is maximum r-scattered?

Theorem

$L(\mathbb{U})$ is maximum r-scattered $\iff$

$$\det \begin{pmatrix} x_1^{q^t} & f_1(x_1) & \cdots & f_r(x_1) \\ x_2^{q^t} & f_1(x_2) & \cdots & f_r(x_2) \\ \vdots & \vdots & & \vdots \\ x_{r+1}^{q^t} & f_1(x_{r+1}) & \cdots & f_r(x_{r+1}) \end{pmatrix} = 0$$

has only solutions $(a_1, \ldots, a_{r+1})$ such that $a_1, \ldots, a_{r+1}$ are $\mathbb{F}_q$-dependent

Monomial case

$f_i(x) = x^{q^{l_j}}$, $t = 0$, $l_1 < \ldots < l_r$

$$F = \det \begin{pmatrix} X_1 & X_1^{q^{l_1}} & \cdots & X_1^{q^{l_r}} \\ X_2 & X_2^{q^{l_1}} & \cdots & X_2^{q^{l_r}} \\ \vdots & \vdots & & \vdots \\ X_{r+1} & X_{r+1}^{q^{l_1}} & \cdots & X_{r+1}^{q^{l_r}} \end{pmatrix},$$

$$G = \det \begin{pmatrix} X_1 & X_1^{q} & \cdots & X_1^{q^{r}} \\ X_2 & X_2^{q} & \cdots & X_2^{q^{r}} \\ \vdots & \vdots & & \vdots \\ X_{r+1} & X_{r+1}^{q} & \cdots & X_{r+1}^{q^{r}} \end{pmatrix}$$

Theorem

$$\mathbb{U} := \{(x, x^{q^{l_1}}, \ldots, x^{q^{l_r}}) : x \in \mathbb{F}_{q^n}\}$$

$L(\mathbb{U})$ is maximum r-scattered if and only if $F/G = 0$ does not contain $\mathbb{F}_{q^n}$-rational points off $G = 0$.

Theorem (B.-Zhou JCTA, 2020)

$I = \{0, i_1, i_2, \ldots, i_r\}$, $0 < i_1 < \cdots < i_r$ *NOT an arithmetic progression.*

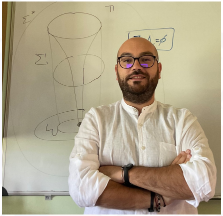
(a) $i_2 - i_0 \neq 2(i_1 - i_0)$;

(b) $i_2 - i_0 = 2(i_1 - i_0)$, $k > 3$ *and* $q \geq 7$;

(c) $i_2 - i_0 = 2(i_1 - i_0)$, $k > 3$, $q = 3, 4, 5$ *and* $i_1 - i_0 > 1$;

(d) $i_2 - i_0 = 2(i_1 - i_0)$, $k > 3$ *and* $q = 2$ *with* $i_1 - i_0 > 2$.

$\exists N$ *such that* $L(\mathbb{U})$ *is not maximum* r*-scattered if* $n > N$

Theorem (B.-Zini-Zullo, IEEE 2023)

$$\mathbb{U} := \{(x^{q^t}, f_1(x), \ldots, f_r(x)) : x \in \mathbb{F}_{q^n}\}$$

$L(\mathbb{U})$ *maximum r-scattered*

- *If* $t = 0$, *and* $(q, \deg_q(f_1(x))) \notin \{(2,2),(2,4),(3,2),(4,2),(5,2)\}$ *then* f_i *is a monomial*
- *If* $t > 0$ *and* $\deg(f_i(x)) > \max\{q^t, \deg(f_1(x))\}$ *for each* $i = 2, \ldots, r$, *then* $f_1(x)$ *is exceptional scattered of index* t.

Tools

$$F(X_1,\dots,X_n,T) = F_0(X_1,\dots,X_n) + F_1(X_1,\dots,X_n)T + \dots + F_d(X_1,\dots,X_n)T^d$$

$$\mathcal{S} : F(X_1,\dots,X_n,T) = 0$$

$F_0(X_1,\dots,X_n)$ has an absolutely irreducible factor non-repeated and $\mathbb{F}_q$-rational

$\Downarrow$

$\mathcal{S}$ contains an absolutely irreducible $\mathbb{F}_q$-rational component

$\mathcal{H}$ hypersurface

$\mathcal{H} \cap \mathcal{S}$ contains an absolutely irreducible non-repeated $\mathbb{F}_q$-rational component

$\Downarrow$

$\mathcal{S}$ contains an absolutely irreducible $\mathbb{F}_q$-rational component

Specific types of RD codes: Minimal RD codes

Definition

$L_{\mathbb{U}}$ linear set of rank n in $\mathrm{PG}(k-1, q^m)$ t-**cutting** $\iff$ $\forall$ $\mathbb{F}_{q^m}$-subspace $H \subset \mathbb{F}_{q^m}^k$ of codimension t $\langle H \cap \mathbb{U} \rangle_{\mathbb{F}_{q^m}} = H$

$t = 1 \implies L_{\mathbb{U}}$ is **(linear) cutting (strong blocking set)**

Theorem

$L_{\mathbb{U}}$ linear set cutting $\iff$ $\mathcal{C}_{\mathbb{U}}$ minimal rank-metric code

Alfarano, Borello, Neri, Ravagnani 2022

Specific types of RD codes: Minimal RD codes

Definition

$L_{\mathbb{U}}$ linear set of rank n in $\mathrm{PG}(k-1, q^m)$ t-**cutting** $\iff$ $\forall$ $\mathbb{F}_{q^m}$-subspace $H \subset \mathbb{F}_{q^m}^k$ of codimension t $\langle H \cap \mathbb{U} \rangle_{\mathbb{F}_{q^m}} = H$

$t = 1 \implies L_{\mathbb{U}}$ is **(linear) cutting (strong blocking set)**

Theorem

$L_{\mathbb{U}}$ *linear set cutting* $\iff$ $\mathcal{C}_{\mathbb{U}}$ *minimal rank-metric code*

Alfarano, Borello, Neri, Ravagnani 2022

Definition

$[n, k]_{q^m/q}$ code $\mathcal{C}$

$v \in \mathcal{C}$ **minimal codeword** $\iff$ $\forall$ $v' \in \mathcal{C}$, $\sigma^{\mathrm{rk}}(v') \subseteq \sigma^{\mathrm{rk}}(v)$ implies $v' = \alpha v$ for some $\alpha \in \mathbb{F}_{q^m}$

$\mathcal{C}$ is **minimal** if all its codewords are minimal

Specific types of RD codes: Minimal RD codes

Definition

$L_{\mathbb{U}}$ linear set of rank n in $\mathrm{PG}(k-1, q^m)$ t-**cutting** $\iff$ $\forall$ $\mathbb{F}_{q^m}$-subspace $H \subset \mathbb{F}_{q^m}^k$ of codimension t $\langle H \cap \mathbb{U} \rangle_{\mathbb{F}_{q^m}} = H$

$t = 1 \implies L_{\mathbb{U}}$ is **(linear) cutting (strong blocking set)**

Theorem

$L_{\mathbb{U}}$ linear set cutting $\iff$ $\mathcal{C}_{\mathbb{U}}$ minimal rank-metric code

Alfarano, Borello, Neri, Ravagnani 2022

See Giuseppe's talk

Specific types of RD codes: Covering RD codes

Definition (Saturating Set)

$S \subset \mathrm{PG}(k-1, q^m)$ ρ-saturating $\iff$ $\forall P \in \mathrm{PG}(k-1, q^m)$ $P \in \langle P_1, \ldots, P_{\rho+1} \rangle$ $P_1, \ldots, P_{\rho+1} \in S$

Theorem

ρ-saturating sets $\iff$ $(\rho + 1)$-covering codes

Specific types of RD codes: Covering RD codes

Definition (Saturating Set)

$$S \subset \mathrm{PG}(k-1, q^m) \text{ } \rho\text{-saturating} \iff \begin{array}{c} \forall P \in \mathrm{PG}(k-1, q^m) \\ P \in \langle P_1, \ldots, P_{\rho+1} \rangle \\ P_1, \ldots, P_{\rho+1} \in S \end{array}$$

Theorem

ρ-saturating sets $\iff$ $(\rho+1)$-covering codes

What if S is a linear set? [Bonini, Borello, and Byrne]

1. construction of saturating linear sets meeting the lower bound
2. link with other properties (scatteredness)
3. When the bound is not tight?

Specific types of RD codes: Covering RD codes

Definition (Saturating Set)

$$S \subset \mathrm{PG}(k-1, q^m) \ \rho\text{-saturating} \iff \begin{array}{c} \forall P \in \mathrm{PG}(k-1, q^m) \\ P \in \langle P_1, \ldots, P_{\rho+1} \rangle \\ P_1, \ldots, P_{\rho+1} \in S \end{array}$$

Theorem

ρ-saturating sets $\iff$ $(\rho+1)$-covering codes

What if S is a linear set? [Bonini, Borello, and Byrne]

1. construction of saturating linear sets meeting the lower bound
2. link with other properties (scatteredness)
3. When the bound is not tight?

See Giuseppe's talk

Indecomposable scattered sequences

Definition (B., Marino,Neri, Vicino 2022)

$i_1, i_2, \ldots, i_m \in \mathbb{N}$
$f_1, \ldots, f_s$ linearized q-polynomials over $\mathbb{F}_{q^n}$ in $\underline{X} = (X_1, \ldots, X_m)$

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

$$\Updownarrow$$

$$\mathbb{U}_{\mathcal{F}} := \left\{ \begin{array}{c} (x_1^{q^{i_1}}, \ldots, x_m^{q^{i_m}}, f_1(\underline{x}), \ldots, f_s(\underline{x})) : \\ \underline{x} = (x_1, \ldots, x_m) \in \mathbb{F}_{q^n}^m \end{array} \right\} \subseteq_{\mathbb{F}_q} \mathbb{F}_{q^n}^{s+m}$$

is maximum h-scattered in $\mathbb{F}_{q^n}^{s+m}$,

Indecomposable scattered sequences

Definition (B. Marino, Neri, Vicino 2022)

$i_1, i_2, \dots, i_m \in \mathbb{N}$

$f_1, \dots, f_s$ linearized q-polynomials over $\mathbb{F}_{q^n}$ in $\underline{X} = (X_1, \dots, X_m)$

$\mathcal{F} := (f_1, \dots, f_s)$ is $(\mathcal{I}; h)_{q^n}$**-scattered sequence** of order m

$$\Updownarrow$$

$$\mathbb{U}_{\mathcal{F}} := \left\{ \begin{array}{c} (x_1^{q^{i_1}}, \dots, x_m^{q^{i_m}}, f_1(\underline{x}), \dots, f_s(\underline{x})) : \\ \underline{x} = (x_1, \dots, x_m) \in \mathbb{F}_{q^n}^m \end{array} \right\} \subseteq_{\mathbb{F}_q} \mathbb{F}_{q^n}^{s+m}$$

is maximum h-scattered in $\mathbb{F}_{q^n}^{s+m}$,

$f(X)$ scattered polynomial of index t $\iff$ $\{(x^{q^t}, f(x)) : x \in \mathbb{F}_{q^n}\} \subseteq_{\mathbb{F}_q} \mathbb{F}_{q^n}^2$ scattered

Sheekey, B.-Zhou

Indecomposable scattered sequences

Definition (B. Marino, Neri, Vicino 2022)

$i_1, i_2, \ldots, i_m \in \mathbb{N}$

$f_1, \ldots, f_s$ linearized q-polynomials over $\mathbb{F}_{q^n}$ in $\underline{X} = (X_1, \ldots, X_m)$

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

$$\Updownarrow$$

$$\mathbb{U}_{\mathcal{F}} := \left\{ \begin{array}{c} (x_1^{q^{i_1}}, \ldots, x_m^{q^{i_m}}, f_1(\underline{x}), \ldots, f_s(\underline{x})) : \\ \underline{x} = (x_1, \ldots, x_m) \in \mathbb{F}_{q^n}^m \end{array} \right\} \subseteq_{\mathbb{F}_q} \mathbb{F}_{q^n}^{s+m}$$

is maximum h-scattered in $\mathbb{F}_{q^n}^{s+m}$,

$f(X)$ scattered polynomial of index t $\iff$ $\{(x^{q^t}, f(x)) : x \in \mathbb{F}_{q^n}\} \subseteq_{\mathbb{F}_q} \mathbb{F}_{q^n}^2$ scattered

Sheekey, B.-Zhou

f is a $(\{t\}, 1)$-scattered sequence of order 1

Indecomposable scattered sequences

Definition (B. Marino, Neri, Vicino 2022)

$i_1, i_2, \ldots, i_m \in \mathbb{N}$

$f_1, \ldots, f_s$ linearized q-polynomials over $\mathbb{F}_{q^n}$ in $\underline{X} = (X_1, \ldots, X_m)$

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

$$\Updownarrow$$

$$\mathbb{U}_{\mathcal{F}} := \left\{ \begin{array}{c} (x_1^{q^{i_1}}, \ldots, x_m^{q^{i_m}}, f_1(\underline{x}), \ldots, f_s(\underline{x})) : \\ \underline{x} = (x_1, \ldots, x_m) \in \mathbb{F}_{q^n}^m \end{array} \right\} \subseteq_{\mathbb{F}_q} \mathbb{F}_{q^n}^{s+m}$$

is maximum h-scattered in $\mathbb{F}_{q^n}^{s+m}$,

$$\mathbb{U} := \{(x^{q^t}, f_1(x), \ldots, f_r(x)) : x \in \mathbb{F}_{q^n}\}$$ maximum r-scattered $\iff$ $f_1, \ldots, f_r$ $(\{t\}, r)$-scattered sequence of order 1

B.-Zhou, B.-Zini-Zullo

Indecomposable scattered sequences

Definition (B., Marino, Neri, Vicino 2022)

$i_1, i_2, \ldots, i_m \in \mathbb{N}$
$f_1, \ldots, f_s$ linearized q-polynomials over $\mathbb{F}_{q^n}$ in $\underline{X} = (X_1, \ldots, X_m)$

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

$$\Updownarrow$$

$$\mathbb{U}_{\mathcal{F}} := \left\{ \begin{array}{c} (x_1^{q^{i_1}}, \ldots, x_m^{q^{i_m}}, f_1(\underline{x}), \ldots, f_s(\underline{x})) : \\ \underline{x} = (x_1, \ldots, x_m) \in \mathbb{F}_{q^n}^m \end{array} \right\} \subseteq_{\mathbb{F}_q} \mathbb{F}_{q^n}^{s+m}$$

is maximum h-scattered in $\mathbb{F}_{q^n}^{s+m}$,

Definition

$(\mathcal{I}; h)_{q^n}$-**scattered sequence** $\mathcal{F} := (f_1, \ldots, f_s)$ of order m is **indecomposable** if it not the direct sum of two smaller scattered sequences

Indecomposable scattered sequences

$$\mathbb{U} := \left\{ \left(x, y, x^q + y^{q^2}, x^{q^2} + y^q + y^{q^2} \right) \;:\; x, y \in \mathbb{F}_{q^4} \right\} \subset \mathbb{F}_{q^4}^4$$

indecomposable $((0,0),1)_{q^4}$-scattered sequence
of order larger than one for $q = 2^{2s+1}$

Indecomposable scattered sequences

$$\mathbb{U} := \left\{ \left(x, y, x^q + y^{q^2}, x^{q^2} + y^q + y^{q^2} \right) \; : \; x, y \in \mathbb{F}_{q^4} \right\} \subset \mathbb{F}_{q^4}^4$$

indecomposable $((0,0),1)_{q^4}$-scattered sequence
of order larger than one for $q = 2^{2s+1}$

Definition

$\alpha, \beta, \gamma \in \mathbb{F}_{q^n}^*$, and $I \neq J \in \mathbb{N}$, $I, J < n-1$

$$\mathbb{U}_{\alpha,\beta,\gamma}^{I,J,n} := \left\{ \left(x, y, x^{q^I} + \alpha y^{q^J}, x^{q^J} + \beta y^{q^I} + \gamma y^{q^J} \right) \; : \; x, y \in \mathbb{F}_{q^n} \right\}.$$

Indecomposable scattered sequences

Theorem

$\gcd(I, J, n) = 1$

$$P^{I,J}_{\alpha,\beta,\gamma}(X) := \begin{cases} X^{q^{J-I}+1} + \gamma X - \alpha\beta, & \text{if } I < J, \\ X^{q^{I-J}+1} + \gamma X^{q^{I-J}} - \alpha\beta, & \text{if } I > J, \end{cases} \tag{1}$$

$P^{I,J}_{\alpha,\beta,\gamma}(X)$ *no roots in* $\mathbb{F}_{q^n} \implies$ $\mathbb{U}^{I,J,n}_{\alpha,\beta,\gamma}$ *exceptional scattered*
$\mathbb{U}^{I,J,n}_{\alpha,\beta,\gamma}$ $(2, 2\max\{I, J\})_q$*-evasive*

Corollary

$P^{I,J}_{\alpha,\beta,\gamma}(X)$ *no roots in* $\mathbb{F}_{q^n}$
$\max\{I, J\} \leq (n-1)/2$
$\implies \mathbb{U}^{I,J,n}_{\alpha,\beta,\gamma}$ *indecomposable cutting exceptional scattered*

Link with algebraic varieties

- $f(x)$ is scattered $\iff$ $rank \begin{pmatrix} x & f(x) \\ y & f(y) \end{pmatrix} = 2$ unless $x = \lambda y$ with $\lambda \in \mathbb{F}_q$

$$\frac{Xf(Y) - Yf(X)}{X^qY - XY^q} = 0 \rightarrow \text{plane curve}$$

Link with algebraic varieties

- $f(x)$ is scattered $\iff$ $rank \begin{pmatrix} x & f(x) \\ y & f(y) \end{pmatrix} = 2$ unless $x = \lambda y$ with $\lambda \in \mathbb{F}_q$

$$\frac{Xf(Y) - Yf(X)}{X^qY - XY^q} = 0 \rightarrow \text{plane curve}$$

- $(x^{q^I} + \alpha y^{q^J}, x^{q^J} + \beta y^{q^I} + \gamma y^{q^J})$ is $((0,0),1)_{q^4}$-scattered sequence

$$\iff rank \begin{pmatrix} x & y & x^{q^I} + \alpha y^{q^J} & x^{q^J} + \beta y^{q^I} + \gamma y^{q^J} \\ z & t & z^{q^I} + \alpha t^{q^J} & z^{q^J} + \beta t^{q^I} + \gamma t^{q^J} \end{pmatrix} = 2$$

unless $(x, y) = \lambda(z, t)$ with $\lambda \in \mathbb{F}_q$

$$\begin{cases} xt - zy = 0 \\ x(z^{q^I} + \alpha t^{q^J}) - z(x^{q^I} + \alpha y^{q^J}) = 0 \\ x(z^{q^J} + \beta t^{q^I} + \gamma t^{q^J}) - z(x^{q^J} + \beta y^{q^I} + \gamma y^{q^J}) = 0 \end{cases} \rightarrow \text{space curve}$$

Scattered sequences: new constructions and infinite families

Definition

$I, J, n, m \in \mathbb{N},\ I < J < n,\ m \geq 3 \qquad \alpha_1, \ldots, \alpha_m \in \mathbb{F}_{q^n}^*$

$$U_{\mathbf{A}}^{I,J} := \{(x_1, \ldots, x_m, x_1^{q^I} + \alpha_2 x_2^{q^J}, \ldots, x_{m-1}^{q^I} + \alpha_m x_m^{q^J}, x_m^{q^I} + \alpha_1 x_1^{q^J}) : x_1, \ldots, x_m \in \mathbb{F}_{q^n}\},$$

where $\mathbf{A} := (\alpha_1, \ldots, \alpha_m)$

Theorem (B.-Giannoni-Marino 2023)

Then the set $U_{\mathbf{A}}^{I,J}$ is exceptional scattered and indecomposable... often

See Alessandro's talk

Maximum 2-scattered linear set

Main open problem about maximum h-scattered in $V(r, q^n)$

Do they exist for every admissible values of r, n and $h \geq 2$?

Maximum 2-scattered linear set

Main open problem about maximum h-scattered in $V(r, q^n)$

Do they exist for every admissible values of r, n and $h \geq 2$?

$2 \mid rn \Longrightarrow \exists$ *maximum 1-scattered linear sets in* $V(r, q^n)$

Ball, Blokhuis, Lavrauw, 2000

Blokhuis, Lavrauw, 2000

Csajbók, Marino, Polverino, Zullo, 2017

B., Giulietti, Marino, Polverino, 2018

Maximum 2-scattered linear set

Main open problem about maximum h-scattered in $V(r, q^n)$
Do they exist for every admissible values of r, n and $h \geq 2$?

$2 \mid rn \implies \exists$ *maximum 1-scattered linear sets in* $V(r, q^n)$

Ball, Blokhuis, Lavrauw, 2000
Blokhuis, Lavrauw, 2000
Csajbók, Marino, Polverino, Zullo, 2017
B., Giulietti, Marino, Polverino, 2018

What about $h = 2$?

1. $r \equiv 0 \pmod 3$ *[Csajbók, Marino, Polverino and Zullo, 2021]*
2. $r = 4$ *and* $n = 3$

Our contribution


$$U := \{(x, y, x^{q^2} + y^q, x^q + y^{q^3}) : x, y \in \mathbb{F}_{q^6}, Tr_{q^6/q^2}(x) = Tr_{q^6/q^2}(y) = 0\}.$$

Proposition

1. *U is 1-scattered*
2. *$W \leq \mathbb{F}_{q^6}^4$ q^2-rational* $\Longrightarrow$ $\dim_{\mathbb{F}_q}(W \cap U)$ *even*
3. *$W \leq \mathbb{F}_{q^6}^4$ q^2-rational hyperplane* $\Longrightarrow$ $\dim_{\mathbb{F}_q}(W' \cap U) \leq 2$ $\forall W' \leq W$ *of dimension 2 and not q^2-rational*

Our contribution


$$U := \{(x, y, x^{q^2} + y^q, x^q + y^{q^3}) : x, y \in \mathbb{F}_{q^6}, Tr_{q^6/q^2}(x) = Tr_{q^6/q^2}(y) = 0\}.$$

Theorem

U is 2-scattered

Our contribution


$$U := \{(x, y, x^{q^2} + y^q, x^q + y^{q^3}) : x, y \in \mathbb{F}_{q^6}, Tr_{q^6/q^2}(x) = Tr_{q^6/q^2}(y) = 0\}.$$

Theorem

U is 2-scattered

1. Case by case analysys
2. Polynomial systems
3. No curves nor varieties :-(
4. $\Longrightarrow \exists$ 2-scattered $V(r, q^6)$ for $r = 4$ and $r \geq 6$

Open questions, future directions

1. Determine whether U is 2-saturating
2. Construct h-scattered linear sets using sequences
3. Find the automorphism groups
4. Find a lower bound on the number of inequivalent examples
5. Generalize U

A.D. 1308 unipg

DIPARTIMENTO
DI MATEMATICA E INFORMATICA

A.D. 1308 unipg

UNIVERSITÀ DEGLI STUDI
DI PERUGIA

13th International Workshop on Coding and Cryptography

WCC 2024

University of Perugia, Italy, June 17–21, 2024
https://wcc2024.sites.dmi.unipg.it

THANK YOU

FOR YOUR ATTENTION