

New maximum scattered linear sets of the projective line

Ferdinando Zullo

joint work with

Bence Csajbók and Giuseppe Marino

Università della Campania “Luigi Vanvitelli”

10–16 September, Irsee

Authors



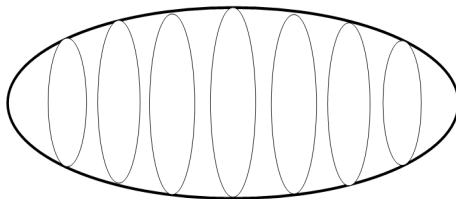
Definition of linear set in $\text{PG}(1, q^n)$

$$\text{PG}(1, q^n) = \text{PG}(W, \mathbb{F}_{q^n}) \quad W = V(2, q^n)$$

Definition of linear set in $\text{PG}(1, q^n)$

$$\text{PG}(1, q^n) = \text{PG}(W, \mathbb{F}_{q^n}) \quad W = V(2, q^n)$$

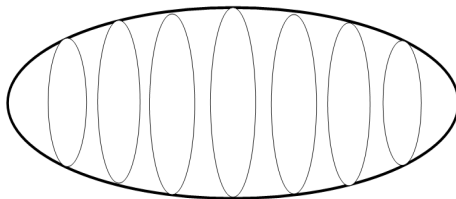
$$W = V(2, q)$$



Definition of linear set in $\text{PG}(1, q^n)$

$$\text{PG}(1, q^n) = \text{PG}(W, \mathbb{F}_{q^n}) \quad W = V(2, q^n)$$

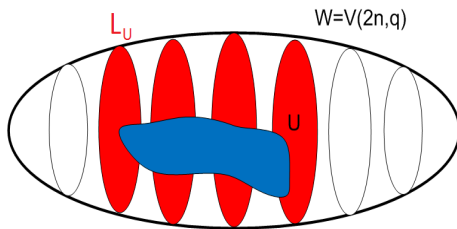
$$W = V(2n, q)$$



$S = \{\langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}} : \mathbf{u} \in W\}$ is a **Desarguesian spread** of W

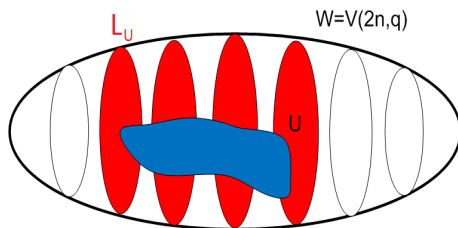
Definition of linear set

U \mathbb{F}_q -subspace of W



Definition of linear set

U \mathbb{F}_q -subspace of W

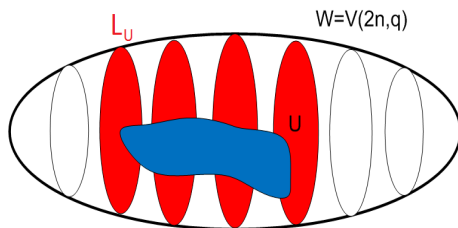


$$L_U = \{ \langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}} : \mathbf{u} \in U \setminus \{ \mathbf{0} \} \}$$

L_U is an \mathbb{F}_q -**linear set** of $PG(1, q^n)$

Definition of linear set

U \mathbb{F}_q -subspace of W



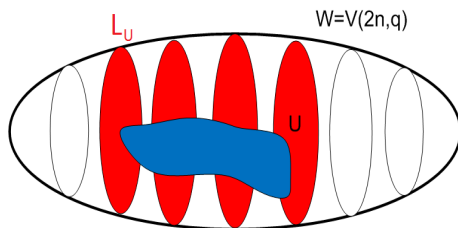
$$L_U = \{ \langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}} : \mathbf{u} \in U \setminus \{ \mathbf{0} \} \}$$

L_U is an \mathbb{F}_q -**linear set** of $PG(1, q^n)$

The **rank** of L_U is $\dim_{\mathbb{F}_q} U$

Definition of linear set

U \mathbb{F}_q -subspace of W



$$L_U = \{ \langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}} : \mathbf{u} \in U \setminus \{0\} \}$$

L_U is an \mathbb{F}_q -**linear set** of $\text{PG}(1, q^n)$

The **rank** of L_U is $\dim_{\mathbb{F}_q} U$

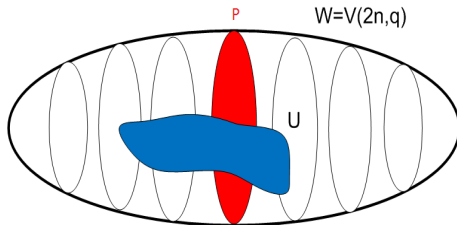
$$\dim_{\mathbb{F}_q} U \leq n$$

The weight of a point

$$P = \langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}} \in \text{PG}(1, q^n)$$

The **weight of P in L_U** is

$$w_{L_U}(P) = \dim_{\mathbb{F}_q}(U \cap \langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}})$$



Maximum scattered linear sets

A linear set L_U of rank k and size $\frac{q^k - 1}{q - 1} \rightarrow$ **scattered linear set**

Maximum scattered linear sets

A linear set L_U of rank k and size $\frac{q^k - 1}{q - 1} \rightarrow$ **scattered linear set**

$$\Leftrightarrow \omega_{L_U}(P) \leq 1 \text{ for each } P \in \text{PG}(1, q^n)$$

Maximum scattered linear sets

A linear set L_U of rank k and size $\frac{q^k - 1}{q - 1} \rightarrow$ **scattered linear set**

$$\Leftrightarrow \omega_{L_U}(P) \leq 1 \text{ for each } P \in \text{PG}(1, q^n)$$

If $k = n \rightarrow$ **maximum scattered linear set of** $\text{PG}(1, q^n)$

Equivalence of linear sets

Equivalence of linear sets

$\phi_f \in \text{P}\Gamma\text{L}(2, q^n)$ defined by $f \in \Gamma\text{L}(2, q^n)$

Equivalence of linear sets

$\phi_f \in \text{P}\Gamma\text{L}(2, q^n)$ defined by $f \in \Gamma\text{L}(2, q^n)$

Definition

L_U and L_V are **equivalent** if there exists a collineation ϕ_f of the line such that $L_U^{\phi_f} = L_{U^f} = L_V$.

Equivalence of linear sets

$\phi_f \in \text{P}\Gamma\text{L}(2, q^n)$ defined by $f \in \Gamma\text{L}(2, q^n)$

Definition

L_U and L_V are **equivalent** if there exists a collineation ϕ_f of the line such that $L_U^{\phi_f} = L_{U^f} = L_V$.

Remark

If $V = U^f$ for some $f \in \Gamma\text{L}(2, q^n) \Rightarrow L_U$ and L_V are equivalent.

Equivalence of linear sets

$\phi_f \in \text{P}\Gamma\text{L}(2, q^n)$ defined by $f \in \Gamma\text{L}(2, q^n)$

Definition

L_U and L_V are **equivalent** if there exists a collineation ϕ_f of the line such that $L_U^{\phi_f} = L_{U^f} = L_V$.

Remark

If $V = U^f$ for some $f \in \Gamma\text{L}(2, q^n) \Rightarrow L_U$ and L_V are equivalent.

The viceversa does **not** hold!

Equivalence of linear sets

$\phi_f \in \text{P}\Gamma\text{L}(2, q^n)$ defined by $f \in \Gamma\text{L}(2, q^n)$

Definition

L_U and L_V are **equivalent** if there exists a collineation ϕ_f of the line such that $L_U^{\phi_f} = L_{U^f} = L_V$.

Remark

If $V = U^f$ for some $f \in \Gamma\text{L}(2, q^n) \Rightarrow L_U$ and L_V are equivalent.

The viceversa does **not** hold!

Example

The linear sets of $\text{PG}(1, q^n)$ of rank $n+1, n+2, \dots, 2n$.

$L_U \mathbb{F}_q$ —linear set of rank n with maximum field of linearity \mathbb{F}_q

L_U \mathbb{F}_q -linear set of rank n with maximum field of linearity \mathbb{F}_q

Γ L-**class** = number of $\Gamma L(2, q^n)$ -orbits on \mathbb{F}_q -subspaces defining L_U

L_U \mathbb{F}_q -linear set of rank n with maximum field of linearity \mathbb{F}_q

Γ L-**class** = number of Γ L($2, q^n$)-orbits on \mathbb{F}_q -subspaces defining L_U

Γ L-class one \rightarrow **simple**

L_U \mathbb{F}_q -linear set of rank n with maximum field of linearity \mathbb{F}_q

Γ L-**class** = number of $\Gamma L(2, q^n)$ -orbits on \mathbb{F}_q -subspaces defining L_U

Γ L-class one \rightarrow **simple**

Giuseppe Marino's talk!

Γ L-class and MRD-codes

If $k = n$

$$L_f = \{ \langle (x, f(x)) \rangle_{\mathbb{F}_{q^n}} : x \in \mathbb{F}_{q^n} \}$$

$$f(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \quad q\text{-polynomial over } \mathbb{F}_{q^n}$$

Γ L-class and MRD-codes

If $k = n$

$$L_f = \{ \langle (x, f(x)) \rangle_{\mathbb{F}_{q^n}} : x \in \mathbb{F}_{q^n} \}$$

$$f(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \quad q\text{-polynomial over } \mathbb{F}_{q^n}$$

If L_f is maximum scattered then

$$\{x \in \mathbb{F}_{q^n} \mapsto ax + bf(x) \in \mathbb{F}_{q^n} : a, b \in \mathbb{F}_{q^n}\}$$

is an **MRD-code**

Γ L-class and MRD-codes

If $k = n$

$$L_f = \{ \langle (x, f(x)) \rangle_{\mathbb{F}_{q^n}} : x \in \mathbb{F}_{q^n} \}$$

$$f(x) = \sum_{i=0}^{n-1} a_i x^{q^i} \quad q\text{-polynomial over } \mathbb{F}_{q^n}$$

If L_f is maximum scattered then

$$\{x \in \mathbb{F}_{q^n} \mapsto ax + bf(x) \in \mathbb{F}_{q^n} : a, b \in \mathbb{F}_{q^n}\}$$

is an **MRD-code**

Γ L-class of L_f = number of inequivalent MRD-codes obtained from L_f

$L_U \mathbb{F}_q$ -linear set of rank n with maximum field of linearity \mathbb{F}_q

$\mathcal{Z}(\Gamma L)$ -class

L_U \mathbb{F}_q -linear set of rank n with maximum field of linearity \mathbb{F}_q

$\mathcal{Z}(\Gamma L)$ -**class** = number of $Z(\Gamma L(2, q^n))$ -orbits on \mathbb{F}_q -subspaces defining L_U

L_U \mathbb{F}_q -linear set of rank n with maximum field of linearity \mathbb{F}_q

$\mathcal{Z}(\Gamma L)$ -**class** = number of $Z(\Gamma L(2, q^n))$ -orbits on \mathbb{F}_q -subspaces defining L_U

$$\Gamma L\text{-class} \leq \mathcal{Z}(\Gamma L)\text{-class}$$

$$\mathrm{PG}(W, \mathbb{F}_{q^n}) = \mathrm{PG}(1, q^n) \rightarrow \mathrm{PG}(W, \mathbb{F}_q) = \mathrm{PG}(2n - 1, q)$$

$$\mathrm{PG}(W, \mathbb{F}_{q^n}) = \mathrm{PG}(1, q^n) \rightarrow \mathrm{PG}(W, \mathbb{F}_q) = \mathrm{PG}(2n-1, q)$$

$$P = \langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}} \in \mathrm{PG}(1, q^n) \rightarrow X_P = \mathrm{PG}(\langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}}, \mathbb{F}_q) = \mathrm{PG}(n-1, q)$$

$$\mathrm{PG}(W, \mathbb{F}_{q^n}) = \mathrm{PG}(1, q^n) \rightarrow \mathrm{PG}(W, \mathbb{F}_q) = \mathrm{PG}(2n-1, q)$$

$$P = \langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}} \in \mathrm{PG}(1, q^n) \rightarrow X_P = \mathrm{PG}(\langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}}, \mathbb{F}_q) = \mathrm{PG}(n-1, q)$$

$$\mathcal{V}(L_U) = \bigcup_{P \in L_U} X_P$$

variety of $\mathrm{PG}(2n-1, q)$ associated to L_U

$$\text{PG}(W, \mathbb{F}_{q^n}) = \text{PG}(1, q^n) \rightarrow \text{PG}(W, \mathbb{F}_q) = \text{PG}(2n-1, q)$$

$$P = \langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}} \in \text{PG}(1, q^n) \rightarrow X_P = \text{PG}(\langle \mathbf{u} \rangle_{\mathbb{F}_{q^n}}, \mathbb{F}_q) = \text{PG}(n-1, q)$$

$$\mathcal{V}(L_U) = \bigcup_{P \in L_U} X_P$$

variety of $\text{PG}(2n-1, q)$ **associated to** L_U

S. Ball, A. Blokhuis and M. Lavrauw: *Linear $(q+1)$ -fold blocking sets in $\text{PG}(2, q^4)$* , Finite Fields Appl., 6 (2000), 294-301.

M. Lavrauw, J. Sheekey and C. Zanella: *On embeddings of minimum dimension of $\text{PG}(n, q) \times \text{PG}(n, q)$* , Des. Codes Cryptogr. 74 n.2 (2015), 427-440.

$\mathcal{H} = PG(V, \mathbb{F}_q) = PG(n-1, q)$ is a **transversal space of** $\mathcal{V}(L_U)$
if $\mathcal{H} \cap X_P \neq \emptyset$ for each $P \in L_U$

$\mathcal{H} = PG(V, \mathbb{F}_q) = PG(n-1, q)$ is a **transversal space of** $\mathcal{V}(L_U)$

if $\mathcal{H} \cap X_P \neq \emptyset$ for each $P \in L_U$

$$\Leftrightarrow L_U = L_V$$

$\mathcal{H} = PG(V, \mathbb{F}_q) = PG(n-1, q)$ is a **transversal space** of $\mathcal{V}(L_U)$
if $\mathcal{H} \cap X_P \neq \emptyset$ for each $P \in L_U$

$$\Leftrightarrow L_U = L_V$$

$\mathcal{Z}(\Gamma L)$ -**class** of L_U = number of **transversal spaces** of $\mathcal{V}(L_U)$ defined by \mathbb{F}_q -spaces not \mathbb{F}_{q^n} -proportional.

$\mathcal{H} = PG(V, \mathbb{F}_q) = PG(n-1, q)$ is a **transversal space** of $\mathcal{V}(L_U)$

if $\mathcal{H} \cap X_P \neq \emptyset$ for each $P \in L_U$

$$\Leftrightarrow L_U = L_V$$

$\mathcal{Z}(\Gamma L)$ -**class** of L_U = number of **transversal spaces** of $\mathcal{V}(L_U)$ defined by \mathbb{F}_q -spaces not \mathbb{F}_{q^n} -proportional.

If L_U is **maximum scattered** \Rightarrow
Number of transversal spaces through $Q \in \mathcal{V}(L_U) = \mathcal{Z}(\Gamma L)$ -class of L_U

Known maximum scattered linear sets: L_1

$$U_1 := \{(x, x^{q^s}) : x \in \mathbb{F}_{q^n}\}$$

$$1 \leq s \leq n-1, \gcd(s, n) = 1$$

Known maximum scattered linear sets: L_1

$$U_1 := \{(x, x^{q^s}) : x \in \mathbb{F}_{q^n}\}$$

$$1 \leq s \leq n-1, \gcd(s, n) = 1$$

found by **Blokhuis and Lavrauw** - 2000

Known maximum scattered linear sets: L_1

$$U_1 := \{(x, x^{q^s}) : x \in \mathbb{F}_{q^n}\}$$

$$1 \leq s \leq n-1, \gcd(s, n) = 1$$

found by **Blokhuis and Lavrauw** - 2000

$$L_1 = \{\langle (x, x^{q^s}) \rangle_{\mathbb{F}_{q^n}} : x \in \mathbb{F}_{q^n}^*\} \rightarrow \text{linear set of pseudoregulus type}$$

Known maximum scattered linear sets: L_1

$$U_1 := \{(x, x^{q^s}) : x \in \mathbb{F}_{q^n}\}$$

$$1 \leq s \leq n-1, \gcd(s, n) = 1$$

found by **Blokhuis and Lavrauw** - 2000

$L_1 = \{\langle (x, x^{q^s}) \rangle_{\mathbb{F}_{q^n}} : x \in \mathbb{F}_{q^n}^*\} \rightarrow$ **linear set of pseudoregulus type**

Classes of L_1

- $\mathcal{Z}(\Gamma L)$ – class = $\varphi(n)$ (**Lavrauw, Sheekey and Zanella** - 2015);
- ΓL – class = $\varphi(n)/2$ (**Csajbók and Zanella** - 2016).

Known maximum scattered linear sets: L_2

$$U_2 = \{(x, \delta x^{q^s} + x^{q^{n-s}}) : x \in \mathbb{F}_{q^n}\}$$

$q \geq 3$, $n \geq 4$, $N_{q^n/q}(\delta) \notin \{0, 1\}$ and $\gcd(s, n) = 1$

Known maximum scattered linear sets: L_2

$$U_2 = \{(x, \delta x^{q^s} + x^{q^{n-s}}) : x \in \mathbb{F}_{q^n}\}$$

$q \geq 3$, $n \geq 4$, $N_{q^n/q}(\delta) \notin \{0, 1\}$ and $\gcd(s, n) = 1$

$s = 1$ found by **Lunardon and Polverino** - 2001

$s > 1$ found by **Sheekey** - 2016

Known maximum scattered linear sets: L_2

$$U_2 = \{(x, \delta x^{q^s} + x^{q^{n-s}}) : x \in \mathbb{F}_{q^n}\}$$

$q \geq 3, n \geq 4, N_{q^n/q}(\delta) \notin \{0, 1\}$ and $\gcd(s, n) = 1$

$s = 1$ found by **Lunardon and Polverino** - 2001

$s > 1$ found by **Sheekey** - 2016

$$L_2 = \{ \langle (x, \delta x^{q^s} + x^{q^{n-s}}) \rangle_{\mathbb{F}_{q^n}} : x \in \mathbb{F}_{q^n}^* \}$$

Theorem (Lunardon-Polverino 2001)

For $q > 3, n \geq 4$ and $s = 1$, L_2 is not equivalent to L_1 .

Known maximum scattered linear sets: L_3

$$U_3 := \{(x, \delta x^{q^s} + x^{q^{s+n/2}}) : x \in \mathbb{F}_{q^n}\}$$

$n \in \{6, 8\}$, $q > 2$, $\gcd(s, n/2) = 1$, $N_{q^n/q^{n/2}}(\delta) \notin \{0, 1\}$ and other conditions on δ and q

Known maximum scattered linear sets: L_3

$$U_3 := \{(x, \delta x^{q^s} + x^{q^{s+n/2}}) : x \in \mathbb{F}_{q^n}\}$$

$n \in \{6, 8\}$, $q > 2$, $\gcd(s, n/2) = 1$, $N_{q^n/q^{n/2}}(\delta) \notin \{0, 1\}$ and other conditions on δ and q

found by **Csajbók, Marino, Polverino and Zanella** - 2017

Known maximum scattered linear sets: L_3

$$U_3 := \{(x, \delta x^{q^s} + x^{q^{s+n/2}}) : x \in \mathbb{F}_{q^n}\}$$

$n \in \{6, 8\}$, $q > 2$, $\gcd(s, n/2) = 1$, $N_{q^n/q^{n/2}}(\delta) \notin \{0, 1\}$ and other conditions on δ and q

found by **Csajbók, Marino, Polverino and Zanella** - 2017

$$L_3 = \{\langle (x, \delta x^{q^s} + x^{q^{s+n/2}}) \rangle_{\mathbb{F}_{q^n}} : x \in \mathbb{F}_{q^n}^*\}$$

Known maximum scattered linear sets: L_3

$$U_3 := \{(x, \delta x^{q^s} + x^{q^{s+n/2}}) : x \in \mathbb{F}_{q^n}\}$$

$n \in \{6, 8\}$, $q > 2$, $\gcd(s, n/2) = 1$, $N_{q^n/q^{n/2}}(\delta) \notin \{0, 1\}$ and other conditions on δ and q

found by **Csajbók, Marino, Polverino and Zanella** - 2017

$$L_3 = \{\langle (x, \delta x^{q^s} + x^{q^{s+n/2}}) \rangle_{\mathbb{F}_{q^n}} : x \in \mathbb{F}_{q^n}^*\}$$

Bence Csajbók's talk!

Our results

Theorem (Csajbók, Marino and FZ)

The linear set $L_2 = \{\langle (x, \delta x^{q^s} + x^{q^{n-s}}) \rangle_{\mathbb{F}_{q^n}} : x \in \mathbb{F}_{q^n}^\}$ is not of pseudoregulus type for each $n \geq 4$, s, δ and $q > 3$.*

Theorem (Csajbók, Marino and FZ)

The linear set $L_2 = \{ \langle (x, \delta x^{q^s} + x^{q^{n-s}}) \rangle_{\mathbb{F}_{q^n}} : x \in \mathbb{F}_{q^n}^ \}$ is not of pseudoregulus type for each $n \geq 4$, s, δ and $q > 3$.*

Theorem (Csajbók, Marino and FZ)

For $n = 6, 8$ and for any choice of the parameters, the linear sets L_1 , L_2 and L_3 are pairwise non-equivalent.

Our results

$$L_4 = \{ \langle (x, x^q + x^{q^3} + bx^{q^5}) \rangle_{\mathbb{F}_{q^6}} : x \in \mathbb{F}_{q^6}^* \}$$

Our results

$$L_4 = \{ \langle (x, x^q + x^{q^3} + bx^{q^5}) \rangle_{\mathbb{F}_{q^6}} : x \in \mathbb{F}_{q^6}^* \}$$

If $q \equiv 0, \pm 1 \pmod{5}$, q odd and $b^2 + b = 1 \Rightarrow L_4$ is a **maximum scattered linear set**!

Our results

$$L_4 = \{ \langle (x, x^q + x^{q^3} + bx^{q^5}) \rangle_{\mathbb{F}_{q^6}} : x \in \mathbb{F}_{q^6}^* \}$$

If $q \equiv 0, \pm 1 \pmod{5}$, q odd and $b^2 + b = 1 \Rightarrow L_4$ is a **maximum scattered linear set**!

- L_4 is **new**;

Our results

$$L_4 = \{ \langle (x, x^q + x^{q^3} + bx^{q^5}) \rangle_{\mathbb{F}_{q^6}} : x \in \mathbb{F}_{q^6}^* \}$$

If $q \equiv 0, \pm 1 \pmod{5}$, q odd and $b^2 + b = 1 \Rightarrow L_4$ is a **maximum scattered linear set**!

- L_4 is **new**;
- it is **simple** if $q \equiv 0 \pmod{5}$;

Our results

$$L_4 = \{ \langle (x, x^q + x^{q^3} + bx^{q^5}) \rangle_{\mathbb{F}_{q^6}} : x \in \mathbb{F}_{q^6}^* \}$$

If $q \equiv 0, \pm 1 \pmod{5}$, q odd and $b^2 + b = 1 \Rightarrow L_4$ is a **maximum scattered linear set**!

- L_4 is **new**;
- it is **simple** if $q \equiv 0 \pmod{5}$;
- **MRD-codes** obtained from L_4 are **new**.

Sketch of the proof

$$L_4 = \{ \langle (x, x^q + x^{q^3} + bx^{q^5}) \rangle_{\mathbb{F}_{q^6}} : x \in \mathbb{F}_{q^6}^* \}$$

is scattered $\Leftrightarrow \omega_{L_4}(P) = 1$ for each $P \in L_4$

Sketch of the proof

$$L_4 = \{ \langle (x, x^q + x^{q^3} + bx^{q^5}) \rangle_{\mathbb{F}_{q^6}} : x \in \mathbb{F}_{q^6}^* \}$$

is **scattered** $\Leftrightarrow \omega_{L_4}(P) = 1$ for each $P \in L_4$

Note that $P \neq \langle (0, 1) \rangle_{\mathbb{F}_{q^6}} \rightarrow P = \langle (1, -m) \rangle_{\mathbb{F}_{q^6}}$ with $m \in \mathbb{F}_{q^6}$.

Sketch of the proof

$$L_4 = \{ \langle (x, x^q + x^{q^3} + bx^{q^5}) \rangle_{\mathbb{F}_{q^6}} : x \in \mathbb{F}_{q^6}^* \}$$

is scattered $\Leftrightarrow \omega_{L_4}(P) = 1$ for each $P \in L_4$

Note that $P \neq \langle (0, 1) \rangle_{\mathbb{F}_{q^6}} \rightarrow P = \langle (1, -m) \rangle_{\mathbb{F}_{q^6}}$ with $m \in \mathbb{F}_{q^6}$.

L_4 is scattered $\Leftrightarrow \frac{x^q + x^{q^3} + bx^{q^5}}{x} = -m$ admits at most q solutions
for each $m \in \mathbb{F}_{q^6}$

Sketch of the proof

$$L_4 = \{ \langle (x, x^q + x^{q^3} + bx^{q^5}) \rangle_{\mathbb{F}_{q^6}} : x \in \mathbb{F}_{q^6}^* \}$$

is **scattered** $\Leftrightarrow \omega_{L_4}(P) = 1$ for each $P \in L_4$

Note that $P \neq \langle (0, 1) \rangle_{\mathbb{F}_{q^6}} \rightarrow P = \langle (1, -m) \rangle_{\mathbb{F}_{q^6}}$ with $m \in \mathbb{F}_{q^6}$.

L_4 is scattered $\Leftrightarrow \frac{x^q + x^{q^3} + bx^{q^5}}{x} = -m$ admits at most q solutions
for each $m \in \mathbb{F}_{q^6}$

$$\Leftrightarrow r(x) = mx + x^q + x^{q^3} + bx^{q^5} \text{ has rank } \geq 5$$

Sketch of the proof

Theorem

The rank of a q -polynomial over \mathbb{F}_{q^n} is equal to the rank of its Dickson matrix.

Sketch of the proof

Theorem

The rank of a q -polynomial over \mathbb{F}_{q^n} is equal to the rank of its Dickson matrix.

Z. **Liu** and B. **Wu**: *Linearized polynomials over finite fields revisited*, Finite Fields Appl. **22** (2013), 79–100.

Sketch of the proof

Theorem

The rank of a q -polynomial over \mathbb{F}_{q^n} is equal to the rank of its Dickson matrix.

Z. Liu and **B. Wu**: *Linearized polynomials over finite fields revisited*, Finite Fields Appl. **22** (2013), 79–100.

$$D = \begin{pmatrix} m & 1 & 0 & 1 & 0 & b \\ b & m^q & 1 & 0 & 1 & 0 \\ 0 & b & m^{q^2} & 1 & 0 & 1 \\ 1 & 0 & b & m^{q^3} & 1 & 0 \\ 0 & 1 & 0 & b & m^{q^4} & 1 \\ 1 & 0 & 1 & 0 & b & m^{q^5} \end{pmatrix}$$

Dickson matrix of $r(x) = mx + x^q + x^{q^3} + bx^{q^5}$

Sketch of the proof

Theorem

The rank of a q -polynomial over \mathbb{F}_{q^n} is equal to the rank of its Dickson matrix.

Z. Liu and **B. Wu**: *Linearized polynomials over finite fields revisited*, Finite Fields Appl. **22** (2013), 79–100.

$$D = \begin{pmatrix} m & 1 & 0 & 1 & 0 & b \\ b & m^q & 1 & 0 & 1 & 0 \\ 0 & b & m^{q^2} & 1 & 0 & 1 \\ 1 & 0 & b & m^{q^3} & 1 & 0 \\ 0 & 1 & 0 & b & m^{q^4} & 1 \\ 1 & 0 & 1 & 0 & b & m^{q^5} \end{pmatrix}$$

Dickson matrix of $r(x) = mx + x^q + x^{q^3} + bx^{q^5}$

L_4 is scattered $\Leftrightarrow \text{rk}(D) \geq 5$ for each $m \in \mathbb{F}_{q^6}$

Sketch of the proof

Theorem

The rank of a q -polynomial over \mathbb{F}_{q^n} is equal to the rank of its Dickson matrix.

Z. Liu and **B. Wu**: *Linearized polynomials over finite fields revisited*, Finite Fields Appl. **22** (2013), 79–100.

$$D = \begin{pmatrix} m & 1 & 0 & 1 & 0 & b \\ b & m^q & 1 & 0 & 1 & 0 \\ 0 & b & m^{q^2} & 1 & 0 & 1 \\ 1 & 0 & b & m^{q^3} & 1 & 0 \\ 0 & 1 & 0 & b & m^{q^4} & 1 \\ 1 & 0 & 1 & 0 & b & m^{q^5} \end{pmatrix}$$

Dickson matrix of $r(x) = mx + x^q + x^{q^3} + bx^{q^5}$

L_4 is scattered $\Leftrightarrow \text{rk}(D) \geq 5$ for each $m \in \mathbb{F}_{q^6}$



Thank you

Thank you for your attention!