Some recent developments in the theory of linear MRD-codes

Olga Polverino

Università degli Studi della Campania, “Luigi Vanvitelli”

Finite Geometries 2017, Fifth Irsee Conference
Irsee

Outline

RD-codes

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

RD-codes

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

$$d(A,B) = rk\,(A-B) \text{ for } A,B \in \mathbb{F}_q^{m\times n}$$

RD-codes

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

$$d(A, B) = rk\,(A - B) \text{ for } A, B \in \mathbb{F}_q^{m \times n}$$

$$\mathcal{C} \subseteq \mathbb{F}_q^{m \times n} \qquad\qquad (\mathcal{C}, d)$$

RD-codes

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

$$d(A,B) = rk\,(A-B) \text{ for } A,B \in \mathbb{F}_q^{m\times n}$$

$\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ $(\mathcal{C}, d)$

Rank Distance Code (RD-code)

RD-codes

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

$$d(A,B) = rk\,(A-B) \text{ for } A,B \in \mathbb{F}_q^{m \times n}$$

$$\mathcal{C} \subseteq \mathbb{F}_q^{m \times n} \qquad (\mathcal{C}, d)$$

Rank Distance Code (RD-code)

$$d(\mathcal{C}) = \min_{A,B \in \mathcal{C},\ A \neq B} \{d(A,B)\}$$

RD-codes

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

$$d(A,B) = rk\,(A-B) \text{ for } A,B \in \mathbb{F}_q^{m\times n}$$

$\mathcal{C} \subseteq \mathbb{F}_q^{m\times n}$ $(\mathcal{C}, d)$

Rank Distance Code (RD-code)

$$d(\mathcal{C}) = \min_{A,B\in\mathcal{C},\ A\neq B} \{d(A,B)\}$$

$d(\mathcal{C})$ *minimum distance* of $\mathcal{C}$

Linear RD-codes

$$\mathcal{C} \quad \rightarrow \quad \mathbb{F}_q\text{-subspace of } \mathbb{F}_q^{m\times n}$$

Linear RD-codes

$\mathcal{C} \quad \rightarrow \quad \mathbb{F}_q$-subspace of $\mathbb{F}_q^{m \times n}$

$\mathcal{C} \quad \mathbb{F}_q$*-linear RD-code*

Linear RD-codes

$$\mathcal{C} \quad \rightarrow \quad \mathbb{F}_q\text{-subspace of } \mathbb{F}_q^{m\times n}$$

$\mathcal{C}$ $\mathbb{F}_q$-*linear RD-code*

$t = \dim_q(\mathcal{C})$

Linear RD-codes

$$\mathcal{C} \quad \rightarrow \quad \mathbb{F}_q\text{-subspace of } \mathbb{F}_q^{m\times n}$$

$$\mathcal{C} \qquad \mathbb{F}_q\textit{-linear RD-code}$$

$$t = \dim_q(\mathcal{C})$$

$$\mathcal{C} \quad \rightarrow \quad [m \times n, t, d]_{\mathbb{F}_q}$$

Linear RD-codes

$$\mathcal{C} \quad \rightarrow \quad \mathbb{F}_q\text{-subspace of } \mathbb{F}_q^{m\times n}$$

$$\mathcal{C} \qquad \mathbb{F}_q\textit{-linear RD-code}$$

$$t = \dim_q(\mathcal{C})$$

$$\mathcal{C} \quad \rightarrow \quad [m \times n, t, d]_{\mathbb{F}_q}$$

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

Linear RD-codes

$\mathcal{C} \quad \rightarrow \quad \mathbb{F}_q$-subspace of $\mathbb{F}_q^{m\times n}$

$\mathcal{C} \quad \mathbb{F}_q$-*linear RD-code*

$t = \dim_q(\mathcal{C})$

$\mathcal{C} \quad \rightarrow \quad [m \times n, t, d]_{\mathbb{F}_q}$

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

Singleton-like bound

Linear RD-codes

$$\mathcal{C} \quad \rightarrow \quad \mathbb{F}_q\text{-subspace of } \mathbb{F}_q^{m\times n}$$

$$\mathcal{C} \qquad \mathbb{F}_q\textit{-linear RD-code}$$

$$t = \dim_q(\mathcal{C})$$

$$\mathcal{C} \quad \rightarrow \quad [m \times n, t, d]_{\mathbb{F}_q}$$

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

Singleton-like bound

P. Delsarte: "Bilinear forms over a finite field, with applications to coding theory", *J. Comb. Theory Ser. A* (1978)

Linear MRD-codes

$\mathcal{C}$ linear RD-code, $[m \times n, t, d]_{\mathbb{F}_q}$

Linear MRD-codes

$\mathcal{C}$ linear RD-code, $[m \times n, t, d]_{\mathbb{F}_q}$

$$t = \max\{m, n\}(\min\{m, n\} - d + 1)$$

Linear MRD-codes

$\mathcal{C}$ linear RD-code, $[m \times n, t, d]_{\mathbb{F}_q}$

$$t = \max\{m, n\}(\min\{m, n\} - d + 1)$$

$\mathcal{C} \quad \rightarrow$ *Maximum Rank Distance* code (MRD-code)

Linear MRD-codes

$\mathcal{C}$ linear RD-code, $[m \times n, t, d]_{\mathbb{F}_q}$

$$t = \max\{m, n\}(\min\{m, n\} - d + 1)$$

$\mathcal{C} \quad \rightarrow \quad$ *Maximum Rank Distance* code (MRD-code)

$$d = 1 \quad \Rightarrow \quad t = m \cdot n \quad \Rightarrow \quad \mathcal{C} = \mathbb{F}_q^{m \times n}$$

Linear MRD-codes

$\mathcal{C}$ linear RD-code, $[m \times n, t, d]_{\mathbb{F}_q}$

$$t = \max\{m, n\}(\min\{m, n\} - d + 1)$$

$\mathcal{C} \quad \rightarrow \quad$ *Maximum Rank Distance* code (MRD-code)

$$d = 1 \quad \Rightarrow \quad t = m \cdot n \quad \Rightarrow \quad \mathcal{C} = \mathbb{F}_q^{m \times n}$$

$$\max\{m, n\} \mid t \quad \rightarrow \quad k = \frac{t}{\max\{m,n\}}$$

Linear MRD-codes

$\mathcal{C}$ linear RD-code, $[m \times n, t, d]_{\mathbb{F}_q}$

$$t = \max\{m,n\}(\min\{m,n\} - d + 1)$$

$\mathcal{C} \quad \rightarrow \quad$ *Maximum Rank Distance* code (MRD-code)

$$d = 1 \quad \Rightarrow \quad t = m \cdot n \quad \Rightarrow \quad \mathcal{C} = \mathbb{F}_q^{m \times n}$$

$$\max\{m,n\} \mid t \quad \rightarrow \quad k = \frac{t}{\max\{m,n\}}$$

$$k = \min\{m,n\} - d + 1$$

Adjoint and dual of MRD-codes

$\mathcal{C}$ linear MRD-code $[m \times n, t, d]_{\mathbb{F}_q}$

Adjoint and dual of MRD-codes

$\mathcal{C}$ linear MRD-code $[m \times n, t, d]_{\mathbb{F}_q}$

$$\Downarrow$$

$\mathcal{C}^T$ linear MRD-code $[n \times m, t, d]_{\mathbb{F}_q}$

Adjoint and dual of MRD-codes

$\mathcal{C}$ linear MRD-code $[m \times n, t, d]_{\mathbb{F}_q}$

$\Downarrow$

$\mathcal{C}^T$ linear MRD-code $[n \times m, t, d]_{\mathbb{F}_q}$

the adjoint code of $\mathcal{C}$

Adjoint and dual of MRD-codes

$\mathcal{C}$ linear MRD-code $[m \times n, t, d]_{\mathbb{F}_q}$

$$\Downarrow$$

$\mathcal{C}^T$ linear MRD-code $[n \times m, t, d]_{\mathbb{F}_q}$

the adjoint code of $\mathcal{C}$

$\mathcal{C}$ linear MRD-code $[m \times n, t, d]_{\mathbb{F}_q}$ $(d > 1)$

Adjoint and dual of MRD-codes

$\mathcal{C}$ linear MRD-code $[m \times n, t, d]_{\mathbb{F}_q}$

$$\Downarrow$$

$\mathcal{C}^T$ linear MRD-code $[n \times m, t, d]_{\mathbb{F}_q}$

the adjoint code of $\mathcal{C}$

$\mathcal{C}$ linear MRD-code $[m \times n, t, d]_{\mathbb{F}_q}$ $(d > 1)$

$$\mathcal{C}^{\perp} = \{M \in \mathbb{F}_q^{m\times n} \,:\, Tr(MN^T) = 0 \; \forall N \in \mathcal{C}\}$$

Adjoint and dual of MRD-codes

$\mathcal{C}$ linear MRD-code $[m \times n, t, d]_{\mathbb{F}_q}$

$$\Downarrow$$

$\mathcal{C}^T$ linear MRD-code $[n \times m, t, d]_{\mathbb{F}_q}$

the adjoint code of $\mathcal{C}$

$\mathcal{C}$ linear MRD-code $[m \times n, t, d]_{\mathbb{F}_q}$ $(d > 1)$

$$\mathcal{C}^\perp = \{M \in \mathbb{F}_q^{m \times n} : Tr(MN^T) = 0 \, \forall N \in \mathcal{C}\}$$

$$\Downarrow$$

$\mathcal{C}^\perp$ MRD-code $[m \times n, mn - t, min\{m, n\} - d + 2]_{\mathbb{F}_q}$

Adjoint and dual of MRD-codes

$$\mathcal{C} \quad \text{linear MRD-code} \quad [m \times n, t, d]_{\mathbb{F}_q}$$

$$\Downarrow$$

$$\mathcal{C}^T \text{ linear MRD-code} \quad [n \times m, t, d]_{\mathbb{F}_q}$$

the adjoint code of $\mathcal{C}$

$$\mathcal{C} \quad \text{linear MRD-code} \quad [m \times n, t, d]_{\mathbb{F}_q} \ (d > 1)$$

$$\mathcal{C}^\perp = \{M \in \mathbb{F}_q^{m \times n} \ : \ Tr(MN^T) = 0 \, \forall N \in \mathcal{C}\}$$

$$\Downarrow$$

$$\mathcal{C}^\perp \text{ MRD-code} \quad [m \times n, mn - t, min\{m,n\} - d + 2]_{\mathbb{F}_q}$$

the Delsarte dual code of $\mathcal{C}$

Equivalence of RD-codes

Equivalence of RD-codes

$\mathcal{C}, \mathcal{C}' \subset \mathbb{F}_q^{m\times n}$ linear RD-codes

Equivalence of RD-codes

$\mathcal{C}, \mathcal{C}' \subset \mathbb{F}_q^{m \times n}$ linear RD-codes

$\mathcal{C}, \mathcal{C}'$ *equivalent*

Equivalence of RD-codes

$\mathcal{C}, \mathcal{C}' \subset \mathbb{F}_q^{m\times n}$ linear RD-codes

$\mathcal{C}, \mathcal{C}'$ *equivalent*

$$\mathcal{C}' = \{AC^\sigma B \,:\, C \in \mathcal{C}\}$$

$A \in GL(m, \mathbb{F}_q)$, $B \in GL(n, \mathbb{F}_q)$ and $\sigma \in Aut(\mathbb{F}_q)$

Equivalence of RD-codes

$\mathcal{C}, \mathcal{C}' \subset \mathbb{F}_q^{m\times n}$ linear RD-codes

$\mathcal{C}, \mathcal{C}'$ *equivalent*

$$\mathcal{C}' = \{AC^\sigma B \,:\, C \in \mathcal{C}\}$$

$A \in GL(m, \mathbb{F}_q)$, $B \in GL(n, \mathbb{F}_q)$ and $\sigma \in Aut(\mathbb{F}_q)$

$Aut(\mathcal{C})$ *Automorphism group* of $\mathcal{C}$

$$Aut(\mathcal{C}) = \{(A, B, \sigma) \in GL(m, q) \times GL(n, q) \times Aut(\mathbb{F}_q) \,:\, A\mathcal{C}^\sigma B = \mathcal{C}\}$$

Left and Right idealiser of RD-codes

$\mathcal{C}$ linear RD-code in $\mathbb{F}_q^{m\times n}$

Left and Right idealiser of RD-codes

$\mathcal{C}$ linear RD-code in $\mathbb{F}_q^{m\times n}$

$$L(\mathcal{C}) = \{Y \in \mathbb{F}_q^{m\times m} : YC \in \mathcal{C} \text{ for all } C \in \mathcal{C}\}$$

Left idealiser of $\mathcal{C}$

Left and Right idealiser of RD-codes

$\mathcal{C}$ linear RD-code in $\mathbb{F}_q^{m\times n}$

$$L(\mathcal{C}) = \{ Y \in \mathbb{F}_q^{m\times m} \ : \ YC \in \mathcal{C} \text{ for all } C \in \mathcal{C}\}$$

Left idealiser of $\mathcal{C}$

$$R(\mathcal{C}) = \{ Z \in \mathbb{F}_q^{n\times n} \ : \ CZ \in \mathcal{C} \text{ for all } C \in \mathcal{C}\}$$

Right idealiser of $\mathcal{C}$

Left and Right idealiser of RD-codes

$\mathcal{C}$ linear RD-code in $\mathbb{F}_q^{m\times n}$

$$L(\mathcal{C}) = \{Y \in \mathbb{F}_q^{m\times m} : YC \in \mathcal{C} \text{ for all } C \in \mathcal{C}\}$$

Left idealiser of $\mathcal{C}$

$$R(\mathcal{C}) = \{Z \in \mathbb{F}_q^{n\times n} : CZ \in \mathcal{C} \text{ for all } C \in \mathcal{C}\}$$

Right idealiser of $\mathcal{C}$

D. Liebhold, G. Nebe: Automorphism groups of Gabidulin-like codes. *Arch. Math.* (2016)

Left and Right idealiser of RD-codes

$\mathcal{C}$ linear RD-code in $\mathbb{F}_q^{m\times n}$

$$L(\mathcal{C}) = \{Y \in \mathbb{F}_q^{m\times m} : YC \in \mathcal{C} \text{ for all } C \in \mathcal{C}\}$$

Left idealiser of $\mathcal{C}$

$$R(\mathcal{C}) = \{Z \in \mathbb{F}_q^{n\times n} : CZ \in \mathcal{C} \text{ for all } C \in \mathcal{C}\}$$

Right idealiser of $\mathcal{C}$

$$L(\mathcal{C})^* \times R(\mathcal{C})^* \times \{id\} \subseteq Aut(\mathcal{C})$$

D. Liebhold, G. Nebe: Automorphism groups of Gabidulin-like codes. *Arch. Math.* (2016)

Left and Right idealiser of MRD-codes

Lunardon-Trombetti-Zhou 2017, JACO

Left and Right idealiser of MRD-codes

Lunardon-Trombetti-Zhou 2017, JACO

- For two equivalent linear metric codes their right (resp. left) idealisers are also equivalent.

Left and Right idealiser of MRD-codes

Lunardon-Trombetti-Zhou 2017, JACO

- For two equivalent linear metric codes their right (resp. left) idealisers are also equivalent.
- Let $\mathcal{C}$ be a linear MRD code in $\mathbb{F}_q^{m\times n}$ with $d > 1$.
  If $m \leq n$ then $L(\mathcal{C})$ is a finite field. Hence $|L(\mathcal{C})| \leq q^m$.
  If $n \leq m$ then $R(\mathcal{C})$ is a finite field. Hence $|R(\mathcal{C})| \leq q^n$.

Left and Right idealiser of MRD-codes

Lunardon-Trombetti-Zhou 2017, JACO

- For two equivalent linear metric codes their right (resp. left) idealisers are also equivalent.
- Let $\mathcal{C}$ be a linear MRD code in $\mathbb{F}_q^{m\times n}$ with $d > 1$.
  If $m \leq n$ then $L(\mathcal{C})$ is a finite field. Hence $|L(\mathcal{C})| \leq q^m$.
  If $n \leq m$ then $R(\mathcal{C})$ is a finite field. Hence $|R(\mathcal{C})| \leq q^n$.
- If $\mathcal{C}$ is a linear MRD code in $\mathbb{F}_q^{n\times n}$ with $d > 1$ then the left and the right idealisers of $\mathcal{C}$ are both finite fields.

Left and Right idealiser of MRD-codes

Lunardon-Trombetti-Zhou 2017, JACO

- For two equivalent linear metric codes their right (resp. left) idealisers are also equivalent.
- Let $\mathcal{C}$ be a linear MRD code in $\mathbb{F}_q^{m\times n}$ with $d > 1$.
  If $m \leq n$ then $L(\mathcal{C})$ is a finite field. Hence $|L(\mathcal{C})| \leq q^m$.
  If $n \leq m$ then $R(\mathcal{C})$ is a finite field. Hence $|R(\mathcal{C})| \leq q^n$.
- If $\mathcal{C}$ is a linear MRD code in $\mathbb{F}_q^{n\times n}$ with $d > 1$ then the left and the right idealisers of $\mathcal{C}$ are both finite fields.

Left and Right idealiser of MRD-codes

Lunardon-Trombetti-Zhou 2017, JACO

- For two equivalent linear metric codes their right (resp. left) idealisers are also equivalent.
- Let $\mathcal{C}$ be a linear MRD code in $\mathbb{F}_q^{m\times n}$ with $d > 1$.
  If $m \leq n$ then $L(\mathcal{C})$ is a finite field. Hence $|L(\mathcal{C})| \leq q^m$.
  If $n \leq m$ then $R(\mathcal{C})$ is a finite field. Hence $|R(\mathcal{C})| \leq q^n$.
- If $\mathcal{C}$ is a linear MRD code in $\mathbb{F}_q^{n\times n}$ with $d > 1$ then the left and the right idealisers of $\mathcal{C}$ are both finite fields.

$\dim_{L(\mathcal{C})}(\mathcal{C}) \quad \dim_{R(\mathcal{C})}(\mathcal{C})$

First Examples of linear MRD-codes

P. Delsarte: Bilinear forms over a finite field, with applications to coding theory, *J. Comb. Theory Ser. A* (1978)

First Examples of linear MRD-codes

P. Delsarte: Bilinear forms over a finite field, with applications to coding theory, *J. Comb. Theory Ser. A* (1978)

E. Gabidulin: Theory of codes with maximum rank distance, *Probl. Inf. Transm.* (1985)

First Examples of linear MRD-codes

P. Delsarte: Bilinear forms over a finite field, with applications to coding theory, *J. Comb. Theory Ser. A* (1978)

E. Gabidulin: Theory of codes with maximum rank distance, *Probl. Inf. Transm.* (1985)

A. Kshevetskiy, E. Gabidulin: The new construction of rank codes, Proceedings ISIT, (2005)

Gabidulin MRD-codes

$$\mathcal{G}_k = \{f(x) = a_0 x + a_1 x^q + \dots a_{k-1} x^{q^{(k-1)}} : a_0, a_1, \dots, a_{k-1} \in \mathbb{F}_{q^n}\},$$

$$n, k \in \mathbb{Z}^+ \quad k < n$$

Gabidulin MRD-codes

$$\mathcal{G}_k = \{f(x) = a_0x + a_1x^q + \dots a_{k-1}x^{q^{(k-1)}} : a_0, a_1, \dots, a_{k-1} \in \mathbb{F}_{q^n}\},$$

$$n, k \in \mathbb{Z}^+ \quad k < n$$

$$dim_{\mathbb{F}_q} Ker\, f \leq k - 1$$

Gabidulin MRD-codes

$$\mathcal{G}_k = \{f(x) = a_0 x + a_1 x^q + \dots a_{k-1} x^{q^{(k-1)}} : a_0, a_1, \dots, a_{k-1} \in \mathbb{F}_{q^n}\},$$

$$n, k \in \mathbb{Z}^+ \quad k < n$$

$$dim_{\mathbb{F}_q} Ker\, f \leq k-1 \quad \Rightarrow \quad dim_{\mathbb{F}_q} Im\, f \geq n-k+1$$

Gabidulin MRD-codes

$$\mathcal{G}_k = \{f(x) = a_0 x + a_1 x^q + \dots a_{k-1} x^{q^{(k-1)}} : a_0, a_1, \dots, a_{k-1} \in \mathbb{F}_{q^n}\},$$

$$n, k \in \mathbb{Z}^+ \quad k < n$$

$$dim_{\mathbb{F}_q} Ker\, f \leq k-1 \quad \Rightarrow \quad dim_{\mathbb{F}_q} Im\, f \geq n-k+1$$

$\mathcal{B}$ $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$ $\rightarrow$ $M_f \in \mathbb{F}_q^{n \times n}$
matrix associated with f w.r.t. $\mathcal{B}$

Gabidulin MRD-codes

$$\mathcal{G}_k = \{f(x) = a_0 x + a_1 x^q + \dots a_{k-1} x^{q^{(k-1)}} : a_0, a_1, \dots, a_{k-1} \in \mathbb{F}_{q^n}\},$$

$$n, k \in \mathbb{Z}^+ \quad k < n$$

$$dim_{\mathbb{F}_q} Ker\, f \leq k-1 \quad \Rightarrow \quad dim_{\mathbb{F}_q} Im\, f \geq n-k+1$$

$\mathcal{B}$ $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$ $\rightarrow$ $M_f \in \mathbb{F}_q^{n\times n}$
matrix associated with f w.r.t. $\mathcal{B}$

$$\mathcal{C}_{\mathcal{G}_k} = \{M_f : f \in \mathcal{G}_k\} \subseteq \mathbb{F}_q^{n\times n},$$

Gabidulin MRD-codes

$$\mathcal{G}_k = \{f(x) = a_0 x + a_1 x^q + \dots a_{k-1} x^{q^{(k-1)}} : a_0, a_1, \dots, a_{k-1} \in \mathbb{F}_{q^n}\},$$

$$n, k \in \mathbb{Z}^+ \quad k < n$$

$$dim_{\mathbb{F}_q} Ker\, f \leq k-1 \quad \Rightarrow \quad dim_{\mathbb{F}_q} Im\, f \geq n-k+1$$

$\mathcal{B}$ $\mathbb{F}_q$-basis of $\mathbb{F}_{q^n}$ $\rightarrow$ $M_f \in \mathbb{F}_q^{n \times n}$
matrix associated with f w.r.t. $\mathcal{B}$

$$\mathcal{C}_{\mathcal{G}_k} = \{M_f : f \in \mathcal{G}_k\} \subseteq \mathbb{F}_q^{n \times n},$$

$\mathcal{C}_{\mathcal{G}_k}$ Gabidulin MRD-code $[n \times n, kn, n-k+1]_{\mathbb{F}_q}$

Gabidulin MRD-codes

$$\mathcal{G}_k = \{f(x) = a_0 x + a_1 x^q + \cdots + a_{k-1} x^{q^{(k-1)}} : a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\},$$

$$n, k \in \mathbb{Z}^+ \quad k < n$$

Gabidulin MRD-codes

$$\mathcal{G}_k = \{f(x) = a_0 x + a_1 x^q + \cdots + a_{k-1} x^{q^{(k-1)}} : a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\},$$

$$n, k \in \mathbb{Z}^+ \quad k < n$$

$U \subseteq \mathbb{F}_{q^n}$, $dim_{\mathbb{F}_q} U = m \leq n$, $\mathcal{B}_U$ basis of U

Gabidulin MRD-codes

$$\mathcal{G}_k = \{f(x) = a_0x + a_1x^q + \cdots + a_{k-1}x^{q^{(k-1)}} : a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\},$$

$$n, k \in \mathbb{Z}^+ \quad k < n$$

$U \subseteq \mathbb{F}_{q^n}$, $dim_{\mathbb{F}_q} U = m \leq n$, $\mathcal{B}_U$ basis of U

$$\mathcal{C}_{\mathcal{G}_k}(U) = \{M_{f_{|U}} : f \in \mathcal{G}_k\} \subseteq \mathbb{F}_q^{n \times m},$$

Gabidulin MRD-codes

$$\mathcal{G}_k = \{f(x) = a_0x + a_1x^q + \cdots + a_{k-1}x^{q^{(k-1)}} : a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\},$$

$$n, k \in \mathbb{Z}^+ \quad k < n$$

$U \subseteq \mathbb{F}_{q^n}$, $dim_{\mathbb{F}_q} U = m \leq n$, $\mathcal{B}_U$ basis of U

$$\mathcal{C}_{\mathcal{G}_k}(U) = \{M_{f_{|U}} : f \in \mathcal{G}_k\} \subseteq \mathbb{F}_q^{n \times m},$$

$\mathcal{C}_{\mathcal{G}_k}(U)$ Gabidulin MRD-code $\quad [n \times m, kn, n-k+1]_{\mathbb{F}_q}$

Gabidulin MRD-codes

$$\mathcal{G}_k = \{f(x) = a_0x + a_1x^q + \cdots + a_{k-1}x^{q^{(k-1)}} : a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\},$$

$$n, k \in \mathbb{Z}^+ \quad k < n$$

$U \subseteq \mathbb{F}_{q^n}$, $dim_{\mathbb{F}_q} U = m \leq n$, $\mathcal{B}_U$ basis of U

$$\mathcal{C}_{\mathcal{G}_k}(U) = \{M_{f_{|U}} \,:\, f \in \mathcal{G}_k\} \subseteq \mathbb{F}_q^{n \times m},$$

$\mathcal{C}_{\mathcal{G}_k}(U)$ Gabidulin MRD-code $[n \times m, kn, n-k+1]_{\mathbb{F}_q}$

$\mathcal{C}_{\mathcal{G}_k}(U)^T$ Gabidulin MRD-code $[m \times n, kn, n-k+1]_{\mathbb{F}_q}$

Generalised Gabidulin MRD-codes

$$\mathcal{G}_{k,s} = \{f(x) = a_0x + a_1x^{q^s} + \cdots + a_{k-1}x^{q^{s(k-1)}} : a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\},$$

$$n, k, s \in \mathbb{Z}^+,\ k < n,\ \gcd(n, s) = 1$$

Generalised Gabidulin MRD-codes

$$\mathcal{G}_{k,s} = \{f(x) = a_0x + a_1x^{q^s} + \cdots + a_{k-1}x^{q^{s(k-1)}} : a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\},$$

$$n, k, s \in \mathbb{Z}^+, k < n, \gcd(n, s) = 1$$

$$\mathcal{C}_{\mathcal{G}_{k,s}} = \{M_f \ : \ f \in \mathcal{G}_k\} \subseteq \mathbb{F}_q^{n \times n},$$

Generalised Gabidulin MRD-codes

$$\mathcal{G}_{k,s} = \{f(x) = a_0x + a_1x^{q^s} + \cdots + a_{k-1}x^{q^{s(k-1)}} : a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\},$$

$$n, k, s \in \mathbb{Z}^+, \, k < n, \, \gcd(n, s) = 1$$

$$\mathcal{C}_{\mathcal{G}_{k,s}} = \{M_f \, : \, f \in \mathcal{G}_k\} \subseteq \mathbb{F}_q^{n \times n},$$

$\mathcal{C}_{\mathcal{G}_{k,s}}$ Generalised Gabidulin MRD-code $[n \times n, kn, n-k+1]_{\mathbb{F}_q}$

Generalised Gabidulin MRD-codes

$$\mathcal{G}_{k,s} = \{f(x) = a_0 x + a_1 x^{q^s} + \cdots + a_{k-1} x^{q^{s(k-1)}} : a_0, a_1, \ldots, a_{k-1} \in \mathbb{F}_{q^n}\},$$

$$n, k, s \in \mathbb{Z}^+,\ k < n,\ \gcd(n, s) = 1$$

$$\mathcal{C}_{\mathcal{G}_{k,s}} = \{M_f\ :\ f \in \mathcal{G}_k\} \subseteq \mathbb{F}_q^{n \times n},$$

$\mathcal{C}_{\mathcal{G}_{k,s}}$	Generalised Gabidulin MRD-code	$[n \times n, kn, n-k+1]_{\mathbb{F}_q}$
$\mathcal{C}_{\mathcal{G}_{k,s}}(U)$	Generalised Gabidulin MRD-code	$[n \times m, kn, n-k+1]_{\mathbb{F}_q}$
$\mathcal{C}_{\mathcal{G}_{k,s}}(U)^T$	Generalised Gabidulin MRD-code	$[m \times n, kn, n-k+1]_{\mathbb{F}_q}$

Linearized polynomials

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

Linearized polynomials

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

$$\downarrow$$

$$End(\mathbb{F}_{q^n}, \mathbb{F}_q)$$

Linearized polynomials

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

$$\downarrow$$

$$End(\mathbb{F}_{q^n}, \mathbb{F}_q)$$

$$\downarrow$$

$$\mathcal{L}_{n,q} = \{f(x) = a_0 x + a_1 x^q + \dots a_{n-1} x^{q^{(n-1)}} : a_0, a_1, \dots, a_{n-1} \in \mathbb{F}_{q^n}\}$$

Linearized polynomials

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

$$\downarrow$$

$$End(\mathbb{F}_{q^n}, \mathbb{F}_q)$$

$$\downarrow$$

$$\mathcal{L}_{n,q} = \{f(x) = a_0 x + a_1 x^q + \dots a_{n-1} x^{q^{(n-1)}} : a_0, a_1, \dots, a_{n-1} \in \mathbb{F}_{q^n}\}$$

$$(\mathcal{L}_{n,q}, +, \circ) \quad \simeq \quad (\mathbb{F}_q^{n\times n}, +, \cdot)$$

Linearized polynomials

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

$$\downarrow$$

$$End(\mathbb{F}_{q^n}, \mathbb{F}_q)$$

$$\downarrow$$

$$\mathcal{L}_{n,q} = \{f(x) = a_0 x + a_1 x^q + \dots a_{n-1} x^{q^{(n-1)}} : a_0, a_1, \dots, a_{n-1} \in \mathbb{F}_{q^n}\}$$

$$(\mathcal{L}_{n,q}, +, \circ) \quad \simeq \quad (\mathbb{F}_q^{n\times n}, +, \cdot)$$

$\circ \quad \rightarrow \quad$ composition modulo $x^{q^n} - x$

Linearized polynomials

$\mathcal{C}, \mathcal{C}' \subseteq \mathcal{L}_{n,q}$ equivalent MRD-codes

Linearized polynomials

$\mathcal{C}, \mathcal{C}' \subseteq \mathcal{L}_{n,q}$ equivalent MRD-codes

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

f, g permutation q-polynomials, $\sigma \in Aut(\mathbb{F}_q)$

Linearized polynomials

$\mathcal{C}, \mathcal{C}' \subseteq \mathcal{L}_{n,q}$ equivalent MRD-codes

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

f, g permutation q-polynomials, $\sigma \in Aut(\mathbb{F}_q)$

$\mathcal{C} \subseteq \mathcal{L}_{n,q}$ MRD-code

Linearized polynomials

$\mathcal{C}, \mathcal{C}' \subseteq \mathcal{L}_{n,q}$ equivalent MRD-codes

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

f, g permutation q-polynomials, $\sigma \in Aut(\mathbb{F}_q)$

$\mathcal{C} \subseteq \mathcal{L}_{n,q}$ MRD-code

$$L(\mathcal{C}) = \{g \in \mathcal{L}_{n,q} \, : \, g \circ f \in \mathcal{C} \text{ for all } f \in \mathcal{C}\}$$

Left idealiser of $\mathcal{C}$

Linearized polynomials

$\mathcal{C}, \mathcal{C}' \subseteq \mathcal{L}_{n,q}$ equivalent MRD-codes

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

f, g permutation q-polynomials, $\sigma \in Aut(\mathbb{F}_q)$

$\mathcal{C} \subseteq \mathcal{L}_{n,q}$ MRD-code

$$L(\mathcal{C}) = \{g \in \mathcal{L}_{n,q} \,:\, g \circ f \in \mathcal{C} \text{ for all } f \in \mathcal{C}\}$$

Left idealiser of $\mathcal{C}$

$$R(\mathcal{C}) = \{h \in \mathcal{L}_{n,q} \,:\, f \circ h \in \mathcal{C} \text{ for all } f \in \mathcal{C}\}$$

Right idealiser of $\mathcal{C}$

Linearized polynomials

$$\mathcal{G}_{k,s} = \{f(x) = a_0 x + a_1 x^{q^s} + \dots a_{k-1} x^{q^{s(k-1)}} : a_0, a_1, \dots, a_{k-1} \in \mathbb{F}_{q^n}\}$$

$$n, k, s \in \mathbb{Z}^+,\ k < n,\ \gcd(n, s) = 1$$

$\mathcal{G}_{k,s}$ Generalised Gabidulin MRD-code $[n \times n, kn, n-k+1]_{\mathbb{F}_q}$

Linearized polynomials

$$\mathcal{G}_{k,s} = \{f(x) = a_0 x + a_1 x^{q^s} + \dots a_{k-1} x^{q^{s(k-1)}} : a_0, a_1, \dots, a_{k-1} \in \mathbb{F}_{q^n}\}$$

$$n, k, s \in \mathbb{Z}^+, \ k < n, \ \gcd(n, s) = 1$$

$\mathcal{G}_{k,s}$ Generalised Gabidulin MRD-code $[n \times n, kn, n-k+1]_{\mathbb{F}_q}$

Linearized polynomials

$$\mathcal{G}_{k,s} = \{f(x) = a_0 x + a_1 x^{q^s} + \dots a_{k-1} x^{q^{s(k-1)}} : a_0, a_1, \dots, a_{k-1} \in \mathbb{F}_{q^n}\}$$

$$n, k, s \in \mathbb{Z}^+, k < n, \gcd(n, s) = 1$$

$\mathcal{G}_{k,s}$ Generalised Gabidulin MRD-code $[n \times n, kn, n - k + 1]_{\mathbb{F}_q}$

$$\mathcal{F}_{q^n} = \{\tau_\alpha(x) = \alpha x \; : \; \alpha \in \mathbb{F}_{q^n}\}$$

Linearized polynomials

$$\mathcal{G}_{k,s} = \{f(x) = a_0x + a_1x^{q^s} + \dots a_{k-1}x^{q^{s(k-1)}} : a_0, a_1, \dots, a_{k-1} \in \mathbb{F}_{q^n}\}$$

$$n, k, s \in \mathbb{Z}^+,\ k < n,\ \gcd(n, s) = 1$$

$\mathcal{G}_{k,s}$ Generalised Gabidulin MRD-code $[n \times n, kn, n-k+1]_{\mathbb{F}_q}$

$$\mathcal{F}_{q^n} = \{\tau_\alpha(x) = \alpha x \ : \ \alpha \in \mathbb{F}_{q^n}\}$$

$$f \circ \tau_\alpha \in \mathcal{G}_{k,s},\ \tau_\alpha \circ f \in \mathcal{G}_{k,s} \quad \text{for all } f \in \mathcal{G}_{k,s},\ \tau_\alpha \in \mathcal{F}_{q^n}$$

Linearized polynomials

$$\mathcal{G}_{k,s} = \{f(x) = a_0 x + a_1 x^{q^s} + \dots a_{k-1} x^{q^{s(k-1)}} : a_0, a_1, \dots, a_{k-1} \in \mathbb{F}_{q^n}\}$$

$$n, k, s \in \mathbb{Z}^+,\ k < n,\ \gcd(n, s) = 1$$

$\mathcal{G}_{k,s}$ Generalised Gabidulin MRD-code $[n \times n, kn, n-k+1]_{\mathbb{F}_q}$

$$\mathcal{F}_{q^n} = \{\tau_\alpha(x) = \alpha x \ : \ \alpha \in \mathbb{F}_{q^n}\}$$

$$f \circ \tau_\alpha \in \mathcal{G}_{k,s},\ \ \tau_\alpha \circ f \in \mathcal{G}_{k,s} \quad \text{for all } \ f \in \mathcal{G}_{k,s},\ \ \tau_\alpha \in \mathcal{F}_{q^n}$$

$$L(\mathcal{G}_{k,s}) = \mathcal{F}_{q^n} \qquad R(\mathcal{G}_{k,s}) = \mathcal{F}_{q^n}$$

Linearized polynomials

$$\mathcal{G}_{k,s} = \{f(x) = a_0 x + a_1 x^{q^s} + \dots a_{k-1} x^{q^{s(k-1)}} : a_0, a_1, \dots, a_{k-1} \in \mathbb{F}_{q^n}\}$$

$$n, k, s \in \mathbb{Z}^+, \; k < n, \; \gcd(n, s) = 1$$

$\mathcal{G}_{k,s}$ Generalised Gabidulin MRD-code $[n \times n, kn, n-k+1]_{\mathbb{F}_q}$

$$\mathcal{F}_{q^n} = \{\tau_\alpha(x) = \alpha x \; : \; \alpha \in \mathbb{F}_{q^n}\}$$

$$f \circ \tau_\alpha \in \mathcal{G}_{k,s}, \;\; \tau_\alpha \circ f \in \mathcal{G}_{k,s} \quad \text{for all} \;\; f \in \mathcal{G}_{k,s}, \;\; \tau_\alpha \in \mathcal{F}_{q^n}$$

$$L(\mathcal{G}_{k,s}) = \mathcal{F}_{q^n} \qquad R(\mathcal{G}_{k,s}) = \mathcal{F}_{q^n}$$

Linearized polynomials

$$\mathcal{G}_{k,s} = \{f(x) = a_0 x + a_1 x^{q^s} + \dots a_{k-1} x^{q^{s(k-1)}} : a_0, a_1, \dots, a_{k-1} \in \mathbb{F}_{q^n}\}$$

$$n, k, s \in \mathbb{Z}^+, \ k < n, \ \gcd(n, s) = 1$$

$\mathcal{G}_{k,s}$ Generalised Gabidulin MRD-code $[n \times n, kn, n-k+1]_{\mathbb{F}_q}$

$$\mathcal{F}_{q^n} = \{\tau_\alpha(x) = \alpha x \ : \ \alpha \in \mathbb{F}_{q^n}\}$$

$$f \circ \tau_\alpha \in \mathcal{G}_{k,s}, \ \tau_\alpha \circ f \in \mathcal{G}_{k,s} \quad \text{for all} \ f \in \mathcal{G}_{k,s}, \ \tau_\alpha \in \mathcal{F}_{q^n}$$

$$L(\mathcal{G}_{k,s}) = \mathcal{F}_{q^n} \qquad R(\mathcal{G}_{k,s}) = \mathcal{F}_{q^n}$$

$\mathcal{G}_{k,s}$ $\mathbb{F}_{q^n}$-linear MRD-code

Finite presemifields

J. De La Cruz, Kiermaier, Wassermann, Willem: Algebraic structures of MRD codes, *Adv. Math. Commun.* (2016)

Finite presemifields

J. De La Cruz, Kiermaier, Wassermann, Willem: Algebraic structures of MRD codes, *Adv. Math. Commun.* (2016)
J. Sheekey: A new family of linear maximum rank distance codes, *Adv. Math. Commun.* (2016)

Finite presemifields

J. De La Cruz, Kiermaier, Wassermann, Willem: Algebraic structures of MRD codes, *Adv. Math. Commun.* (2016)
J. Sheekey: A new family of linear maximum rank distance codes, *Adv. Math. Commun.* (2016)

$\mathcal{C}$ $\mathbb{F}_q$-linear MRD-code, $[n \times n, n, n]_{\mathbb{F}_q}$

$$\updownarrow$$

$\mathcal{S}_\mathcal{C}$ presemifield of order q^n with left nucleus containing $\mathbb{F}_q$

Finite presemifields

J. De La Cruz, Kiermaier, Wassermann, Willem: Algebraic structures of MRD codes, *Adv. Math. Commun.* (2016)
J. Sheekey: A new family of linear maximum rank distance codes, *Adv. Math. Commun.* (2016)

$\mathcal{C}$ $\mathbb{F}_q$-linear MRD-code, $[n \times n, n, n]_{\mathbb{F}_q}$

$\updownarrow$

$\pi_{\mathcal{S}_{\mathcal{C}}}$ semifield plane of order q^n

Finite presemifields

J. De La Cruz, Kiermaier, Wassermann, Willem: Algebraic structures of MRD codes, *Adv. Math. Commun.* (2016)
J. Sheekey: A new family of linear maximum rank distance codes, *Adv. Math. Commun.* (2016)

$$\mathcal{C} \quad \mathbb{F}_q\text{-linear MRD-code,} \quad [n \times n, n, n]_{\mathbb{F}_q}$$

$$\updownarrow$$

$\pi_{\mathcal{S}_{\mathcal{C}}}$ semifield plane of order q^n

$$\mathcal{G}_{1,s} \quad \rightarrow \quad \mathcal{S}_{\mathcal{G}_{1,s}} \text{ isotopic to } \mathbb{F}_{q^n}$$

Finite presemifields

J. De La Cruz, Kiermaier, Wassermann, Willem: Algebraic structures of MRD codes, *Adv. Math. Commun.* (2016)
J. Sheekey: A new family of linear maximum rank distance codes, *Adv. Math. Commun.* (2016)

$\mathcal{C}$ $\mathbb{F}_q$-linear MRD-code, $[n \times n, n, n]_{\mathbb{F}_q}$

$$\updownarrow$$

$\pi_{\mathcal{S}_\mathcal{C}}$ semifield plane of order q^n

$\mathcal{G}_{1,s} \quad \rightarrow \quad \pi_{\mathcal{S}_{\mathcal{G}_{1,s}}}$ Desarguesian plane

Generalized Twisted Gabidulin Codes

Sheekey, 2016

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

$$n, k, s \in \mathbb{Z}^+, \quad k < n, \quad gcd(n, s) = 1, \quad N_q(\eta) \neq (-1)^{nk}$$

Generalized Twisted Gabidulin Codes

Sheekey, 2016

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

$$n, k, s \in \mathbb{Z}^+, \quad k < n, \quad gcd(n, s) = 1, \quad N_q(\eta) \neq (-1)^{nk}$$

Generalized Twisted Gabidulin Codes

Sheekey, 2016

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

$$n, k, s \in \mathbb{Z}^+, \quad k < n, \quad gcd(n, s) = 1, \quad N_q(\eta) \neq (-1)^{nk}$$

$$\mathcal{H}_{k,s}(\eta, h) \qquad \text{MRD-code} \quad [n \times n, kn, n-k+1]_{\mathbb{F}_q}$$

Generalized Twisted Gabidulin Codes

Sheekey, 2016

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

$$n, k, s \in \mathbb{Z}^+, \quad k < n, \quad gcd(n, s) = 1, \quad N_q(\eta) \neq (-1)^{nk}$$

$$\mathcal{H}_{k,s}(\eta, h) \qquad \text{MRD-code} \quad [n \times n, kn, n-k+1]_{\mathbb{F}_q}$$

$$\mathcal{H}_{k,s}(0, h) = \mathcal{G}_{k,s}$$

Generalized Twisted Gabidulin Codes

Sheekey, 2016

$$\mathcal{H}_{k,s}(\eta,h)=\{f(x)=a_0x+a_1x^{q^s}+\cdots+a_{k-1}x^{q^{s(k-1)}}+\eta a_0^{q^h}x^{q^{sk}}\ :\ a_i\in\mathbb{F}_{q^n}\}$$

$$n,k,s\in\mathbb{Z}^+,\quad k<n,\quad gcd(n,s)=1,\quad N_q(\eta)\neq(-1)^{nk}$$

$\mathcal{H}_{k,s}(\eta,h)$ MRD-code $[n\times n,kn,n-k+1]_{\mathbb{F}_q}$

$$\mathcal{H}_{k,s}(0,h)=\mathcal{G}_{k,s}$$

$\mathcal{H}_{1,s}(\eta,h)\ \rightarrow\ a_0x+\eta a_0^{q^h}x^{q^s}$ Generalized twisted field

Generalized Twisted Gabidulin Codes

Sheekey, 2016

$$\mathcal{H}_{k,s}(\eta,h)=\{f(x)=a_0x+a_1x^{q^s}+\cdots+a_{k-1}x^{q^{s(k-1)}}+\eta a_0^{q^h}x^{q^{sk}}\ :\ a_i\in\mathbb{F}_{q^n}\}$$

$$n,k,s\in\mathbb{Z}^+,\quad k<n,\quad gcd(n,s)=1,\quad N_q(\eta)\neq(-1)^{nk}$$

$\mathcal{H}_{k,s}(\eta,h)$ MRD-code $[n\times n, kn, n-k+1]_{\mathbb{F}_q}$

$$\mathcal{H}_{k,s}(0,h)=\mathcal{G}_{k,s}$$

$\mathcal{H}_{1,s}(\eta,h) \quad\rightarrow\quad a_0x+\eta a_0^{q^h}x^{q^s}$ Generalized twisted field

$$\mathcal{H}_2(\eta,1)$$

K. Otal, F. Özbudak: Explicit Construction of Some Non-Gabidulin Linear Maximum Rank Distance Codes, *Adv. Math. Commun.* (2016)

Generalized Twisted Gabidulin Codes

Sheekey 2016/ Lunardon-Trombetti-Zhou, ArXiv (2015)

Generalized Twisted Gabidulin Codes

Sheekey 2016/ Lunardon-Trombetti-Zhou, ArXiv (2015)

- If $\eta \neq 0$, then $\mathcal{H}_{k,s}(\eta, h) \not\simeq \mathcal{G}_{k,s}$ unless $k \in \{1, n-1\}$ and $h \in \{0, 1\}$.

Generalized Twisted Gabidulin Codes

Sheekey 2016/ Lunardon-Trombetti-Zhou, ArXiv (2015)

- If $\eta \neq 0$, then $\mathcal{H}_{k,s}(\eta, h) \not\simeq \mathcal{G}_{k,s}$ unless $k \in \{1, n-1\}$ and $h \in \{0, 1\}$.

Lunardon-Trombetti-Zhou (2017),JACO

Generalized Twisted Gabidulin Codes

Sheekey 2016/ Lunardon-Trombetti-Zhou, ArXiv (2015)

- If $\eta \neq 0$, then $\mathcal{H}_{k,s}(\eta, h) \not\simeq \mathcal{G}_{k,s}$ unless $k \in \{1, n-1\}$ and $h \in \{0, 1\}$.

Lunardon-Trombetti-Zhou (2017),JACO

$$\mathcal{H}_{k,s}(\eta, h)$$

Generalized Twisted Gabidulin Codes

Sheekey 2016/ Lunardon-Trombetti-Zhou, ArXiv (2015)

- If $\eta \neq 0$, then $\mathcal{H}_{k,s}(\eta, h) \not\simeq \mathcal{G}_{k,s}$ unless $k \in \{1, n-1\}$ and $h \in \{0, 1\}$.

Lunardon-Trombetti-Zhou (2017),JACO

$$\mathcal{H}_{k,s}(\eta, h)$$

- If $\eta = 0$, then $\mathcal{H}_{k,s}(0, h) = \mathcal{G}_{k,s}$ and $L(\mathcal{G}_{k,s}) = R(\mathcal{G}_{k,s}) \simeq \mathbb{F}_{q^n}$.

Generalized Twisted Gabidulin Codes

Sheekey 2016/ Lunardon-Trombetti-Zhou, ArXiv (2015)

- If $\eta \neq 0$, then $\mathcal{H}_{k,s}(\eta, h) \not\simeq \mathcal{G}_{k,s}$ unless $k \in \{1, n-1\}$ and $h \in \{0, 1\}$.

Lunardon-Trombetti-Zhou (2017),JACO

$$\mathcal{H}_{k,s}(\eta, h)$$

- If $\eta = 0$, then $\mathcal{H}_{k,s}(0, h) = \mathcal{G}_{k,s}$ and $L(\mathcal{G}_{k,s}) = R(\mathcal{G}_{k,s}) \simeq \mathbb{F}_{q^n}$.
- If $\eta \neq 0$ and $1 < k < n-1$, then $L(\mathcal{H}_{k,s}(\eta, h)) \simeq \mathbb{F}_{q^{gcd(n,h)}}$ and $R(\mathcal{H}_{k,s}(\eta, h)) \simeq \mathbb{F}_{q^{gcd(n,sk-h)}}$.

Subfamilies of $\mathcal{H}$

$$\mathcal{H} = \{\mathcal{H}_{k,s}(\eta, h) \subseteq \mathcal{L}_{n,q}\}$$

Subfamilies of $\mathcal{H}$

$$\mathcal{H} = \{\mathcal{H}_{k,s}(\eta, h) \subseteq \mathcal{L}_{n,q}\}$$

$$\mathcal{G} = \{\mathcal{G}_{k,s} \subseteq \mathcal{L}_{n,q}\}$$

Subfamilies of $\mathcal{H}$

$$\mathcal{H} = \{\mathcal{H}_{k,s}(\eta, h) \subseteq \mathcal{L}_{n,q}\}$$

$$\mathcal{G} = \{\mathcal{G}_{k,s} \subseteq \mathcal{L}_{n,q}\}$$

$$\mathcal{H}_L = \{\mathcal{C} \in \mathcal{H} \; : \; L(\mathcal{C}) \simeq \mathbb{F}_{q^n}\}$$

$$\mathcal{H}_R = \{\mathcal{C} \in \mathcal{H} \; : \; R(\mathcal{C}) \simeq \mathbb{F}_{q^n}\}$$

Subfamilies of $\mathcal{H}$

$$\mathcal{H} = \{\mathcal{H}_{k,s}(\eta, h) \subseteq \mathcal{L}_{n,q}\}$$

$$\mathcal{G} = \{\mathcal{G}_{k,s} \subseteq \mathcal{L}_{n,q}\}$$

$$\mathcal{H}_L = \{\mathcal{C} \in \mathcal{H} \,:\, L(\mathcal{C}) \simeq \mathbb{F}_{q^n}\}$$

$$\mathcal{H}_R = \{\mathcal{C} \in \mathcal{H} \,:\, R(\mathcal{C}) \simeq \mathbb{F}_{q^n}\}$$

$$\mathcal{G} = \mathcal{H}_R \cap \mathcal{H}_L$$

Subfamilies of $\mathcal{H}$

$$\mathcal{H} = \{\mathcal{H}_{k,s}(\eta, h) \subseteq \mathcal{L}_{n,q}\}$$

$$\mathcal{G} = \{\mathcal{G}_{k,s} \subseteq \mathcal{L}_{n,q}\}$$

$$\mathcal{H}_L = \{\mathcal{C} \in \mathcal{H} \; : \; L(\mathcal{C}) \simeq \mathbb{F}_{q^n}\}$$

$$\mathcal{H}_R = \{\mathcal{C} \in \mathcal{H} \; : \; R(\mathcal{C}) \simeq \mathbb{F}_{q^n}\}$$

$$\mathcal{G} = \mathcal{H}_R \cap \mathcal{H}_L$$

$$\mathcal{G} \subset \mathcal{H}_L \subset \mathcal{H}$$

$$\mathcal{G} \subset \mathcal{H}_R \subset \mathcal{H}$$

Subfamilies of $\mathcal{M}$

$$\mathcal{M} = \{\mathcal{C} \subset \mathcal{L}_{n,q} : \mathcal{C}\ MRD-code, d > 1\}$$

Subfamilies of $\mathcal{M}$

$$\mathcal{M} = \{\mathcal{C} \subset \mathcal{L}_{n,q} \, : \, \mathcal{C} \, MRD - code, d > 1\}$$

$$\mathcal{M}_{L,R} = \{\mathcal{C} \in \mathcal{M} \, : \, L(\mathcal{C}), R(\mathcal{C}) \simeq \mathbb{F}_{q^n}\}$$

$$\mathcal{M}_{L} = \{\mathcal{C} \in \mathcal{M} \, : \, L(\mathcal{C}) \simeq \mathbb{F}_{q^n}\}$$

$$\mathcal{M}_{R} = \{\mathcal{C} \in \mathcal{M} \, : \, R(\mathcal{C}) \simeq \mathbb{F}_{q^n}\}$$

$$\mathcal{M}_{L,R} \subset \mathcal{M}_{L} \subset \mathcal{M}$$

Subfamilies of $\mathcal{M}$

$$\mathcal{M} = \{\mathcal{C} \subset \mathcal{L}_{n,q} \,:\, \mathcal{C}\; MRD - code, d > 1\}$$

$$\mathcal{M}_{L,R} = \{\mathcal{C} \in \mathcal{M} \,:\, L(\mathcal{C}), R(\mathcal{C}) \simeq \mathbb{F}_{q^n}\}$$

$$\mathcal{M}_{L} = \{\mathcal{C} \in \mathcal{M} \,:\, L(\mathcal{C}) \simeq \mathbb{F}_{q^n}\}$$

$$\mathcal{M}_{R} = \{\mathcal{C} \in \mathcal{M} \,:\, R(\mathcal{C}) \simeq \mathbb{F}_{q^n}\}$$

$$\mathcal{M}_{L,R} \subset \mathcal{M}_{L} \subset \mathcal{M}$$

The family $\mathcal{M}_L$

$\mathcal{M}_L \quad \leftrightarrow \quad$ MRD-codes $\mathbb{F}_{q^n}$-linear

The family $\mathcal{M}_L$

$$\mathcal{M}_L \quad \leftrightarrow \quad \text{MRD-codes } \mathbb{F}_{q^n}\text{-linear}$$

$$\mathcal{C} \in \mathcal{M}_L \quad \Longrightarrow \quad \exists\ \mathcal{C}' \simeq \mathcal{C} \text{ such that } L(\mathcal{C}') = \mathcal{F}_{q^n}$$

The family $\mathcal{M}_L$

$$\mathcal{M}_L \quad \leftrightarrow \quad \text{MRD-codes } \mathbb{F}_{q^n}\text{-linear}$$

$$\mathcal{C} \in \mathcal{M}_L \quad \Longrightarrow \quad \exists\ \mathcal{C}' \simeq \mathcal{C} \text{ such that } L(\mathcal{C}') = \mathcal{F}_{q^n}$$

$$\mathcal{G} \subset \mathcal{H}_L \subseteq \mathcal{M}_L$$

The family $\mathcal{M}_L$

$$\mathcal{M}_L \quad \leftrightarrow \quad \text{MRD-codes } \mathbb{F}_{q^n}\text{-linear}$$

$$\mathcal{C} \in \mathcal{M}_L \quad \Longrightarrow \quad \exists\ \mathcal{C}' \simeq \mathcal{C} \text{ such that } L(\mathcal{C}') = \mathcal{F}_{q^n}$$

$$\mathcal{G} \subset \mathcal{H}_L \subseteq \mathcal{M}_L$$

Horlemann-Trautmann, Marshall: New Criteria for MRD and Gabidulin Codes and some Rank-Metric Code Constructions, arXiv:1507.08641v3 (2016)

MRD-codes and maximum scattered spaces

Sheekey, AMC (2016)

MRD-codes and maximum scattered spaces

Sheekey, AMC (2016)

$$\mathcal{C} \in \mathcal{M}_L, \quad k = 2$$

MRD-codes and maximum scattered spaces

Sheekey, AMC (2016)

$$\mathcal{C} \in \mathcal{M}_L, \quad k = 2$$

$$\mathcal{C} \text{ MRD-code}, \quad [n \times n, 2n, n-1]_{\mathbb{F}_q}, \quad L(\mathcal{C}) = \mathcal{F}_{q^n}$$

$$\mathcal{C} \simeq \mathcal{C}_f = [x, f(x)]_{\mathcal{F}_{q^n}}$$

MRD-codes and maximum scattered spaces

Sheekey, AMC (2016)

$$\mathcal{C} \in \mathcal{M}_L, \quad k = 2$$

$\mathcal{C}$ MRD-code, $\quad [n \times n, 2n, n-1]_{\mathbb{F}_q}, \quad L(\mathcal{C}) = \mathcal{F}_{q^n}$

$$\mathcal{C} \simeq \mathcal{C}_f = [x, f(x)]_{\mathcal{F}_{q^n}}$$

$$\updownarrow$$

MRD-codes and maximum scattered spaces

Sheekey, AMC (2016)

$$\mathcal{C} \in \mathcal{M}_L, \quad k = 2$$

$\mathcal{C}$ MRD-code, $\quad [n \times n, 2n, n-1]_{\mathbb{F}_q}, \quad L(\mathcal{C}) = \mathcal{F}_{q^n}$

$$\mathcal{C} \simeq \mathcal{C}_f = [x, f(x)]_{\mathcal{F}_{q^n}}$$

$$\updownarrow$$

$\Phi_f(x) = \frac{f(x)}{x}$

MRD-codes and maximum scattered spaces

Sheekey, AMC (2016)

$$\mathcal{C} \in \mathcal{M}_L, \quad k = 2$$

$$\mathcal{C} \text{ MRD-code}, \quad [n \times n, 2n, n-1]_{\mathbb{F}_q}, \quad L(\mathcal{C}) = \mathcal{F}_{q^n}$$

$$\mathcal{C} \simeq \mathcal{C}_f = [x, f(x)]_{\mathcal{F}_{q^n}}$$

$$\updownarrow$$

$$\Phi_f(x) = \frac{f(x)}{x} \quad \longrightarrow \quad |Im(\Phi_f)| = q^{n-1} + q^{n-2} + \cdots + q + 1$$

MRD-codes and maximum scattered spaces

Sheekey, AMC (2016)

$$\mathcal{C} \in \mathcal{M}_L, \quad k = 2$$

$$\mathcal{C} \text{ MRD-code}, \quad [n \times n, 2n, n-1]_{\mathbb{F}_q}, \quad L(\mathcal{C}) = \mathcal{F}_{q^n}$$

$$\mathcal{C} \simeq \mathcal{C}_f = [x, f(x)]_{\mathcal{F}_{q^n}}$$

$$\updownarrow$$

$$U_f = \{(x, f(x)) \,:\, x \in \mathbb{F}_{q^n}\} \subset V = \mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$$

MRD-codes and maximum scattered spaces

Sheekey, AMC (2016)

$$\mathcal{C} \in \mathcal{M}_L, \quad k = 2$$

$\mathcal{C}$ MRD-code, $\quad [n \times n, 2n, n-1]_{\mathbb{F}_q}, \quad L(\mathcal{C}) = \mathcal{F}_{q^n}$

$$\mathcal{C} \simeq \mathcal{C}_f = [x, f(x)]_{\mathcal{F}_{q^n}}$$

$$\updownarrow$$

$$U_f = \{(x, f(x)) \, : \, x \in \mathbb{F}_{q^n}\} \subset V = \mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$$

Maximum Scattered Space of V

Maximum scattered spaces-Maximum scattered linear sets

U $\mathbb{F}_q$-subspace of $\mathbb{V} = V(r, q^n)$, with $\mathbb{F}_q$-dimension k

Maximum scattered spaces-Maximum scattered linear sets

U $\mathbb{F}_q$-subspace of $\mathbb{V} = V(r, q^n)$, with $\mathbb{F}_q$-dimension k

Definition

Maximum scattered spaces-Maximum scattered linear sets

U $\mathbb{F}_q$-subspace of $\mathbb{V} = V(r, q^n)$, with $\mathbb{F}_q$-dimension k

Definition

- U is a scattered $\mathbb{F}_q$-subspace of $\mathbb{V}$ if

$$dim_{\mathbb{F}_q}(U \cap [\underline{v}]_{\mathbb{F}_{q^n}}) \leq 1$$

for all $\underline{v} \in \mathbb{V}$.

Maximum scattered spaces-Maximum scattered linear sets

U $\mathbb{F}_q$-subspace of $\mathbb{V} = V(r, q^n)$, with $\mathbb{F}_q$-dimension k

Definition

- U is a scattered $\mathbb{F}_q$-subspace of $\mathbb{V}$ if

$$dim_{\mathbb{F}_q}(U \cap [\underline{v}]_{\mathbb{F}_{q^n}}) \leq 1$$

for all $\underline{v} \in \mathbb{V}$.

U is a $\mathbb{F}_q$-scattered subspace if

$$|L_U| = q^{k-1} + q^{k-2} + \cdots + q + 1 \text{ where } L_U \subset PG(\mathbb{V})$$

Maximum scattered spaces-Maximum scattered linear sets

U $\mathbb{F}_q$-subspace of $\mathbb{V} = V(r, q^n)$, with $\mathbb{F}_q$-dimension k

Definition

- U is a scattered $\mathbb{F}_q$-subspace of $\mathbb{V}$ if

$$dim_{\mathbb{F}_q}(U \cap [\underline{v}]_{\mathbb{F}_{q^n}}) \leq 1$$

for all $\underline{v} \in \mathbb{V}$.

U is a $\mathbb{F}_q$-scattered subspace if

$|L_U| = q^{k-1} + q^{k-2} + \cdots + q + 1$ where $L_U \subset PG(\mathbb{V})$

L_U scattered $\mathbb{F}_q$-linear set

Maximum scattered spaces-Maximum scattered linear sets

U $\mathbb{F}_q$-subspace of $\mathbb{V} = V(r, q^n)$, with $\mathbb{F}_q$-dimension k

Definition

- U is a scattered $\mathbb{F}_q$-subspace of $\mathbb{V}$ if
$$dim_{\mathbb{F}_q}(U \cap [\underline{v}]_{\mathbb{F}_{q^n}}) \leq 1$$
for all $\underline{v} \in \mathbb{V}$.
U is a $\mathbb{F}_q$-scattered subspace if
$$|L_U| = q^{k-1} + q^{k-2} + \cdots + q + 1 \text{ where } L_U \subset PG(\mathbb{V})$$
L_U scattered $\mathbb{F}_q$-linear set
- U is a Maximum Scattered $\mathbb{F}_q$-subspace of $\mathbb{V}$ if $dim_{\mathbb{F}_q} U$ is the highest possible dimension of a scattered $\mathbb{F}_q$-subspace of $\mathbb{V}$

Maximum scattered spaces-Maximum scattered linear sets

$U \quad \mathbb{F}_q$-subspace of $\mathbb{V} = V(r, q^n)$, with $\mathbb{F}_q$-dimension k

Definition

- U is a scattered $\mathbb{F}_q$-subspace of $\mathbb{V}$ if
$$dim_{\mathbb{F}_q}(U \cap [\underline{v}]_{\mathbb{F}_{q^n}}) \leq 1$$
for all $\underline{v} \in \mathbb{V}$.
U is a $\mathbb{F}_q$-scattered subspace if
$$|L_U| = q^{k-1} + q^{k-2} + \cdots + q + 1 \text{ where } L_U \subset PG(\mathbb{V})$$
L_U scattered $\mathbb{F}_q$-linear set
- U is a Maximum Scattered $\mathbb{F}_q$-subspace of $\mathbb{V}$ if $dim_{\mathbb{F}_q} U$ is the highest possible dimension of a scattered $\mathbb{F}_q$-subspace of $\mathbb{V}$

A. Blokhuis, M. Lavrauw: *Scattered spaces with respect to a spread in PG(n,q)*, Geom. Dedicata (2000)

Maximum Scattered Spaces

Blokhuis-Lavrauw 2000

Maximum Scattered Spaces

Blokhuis-Lavrauw 2000

- $U \subset \mathbb{V} = V(r, q^n)$ scattered $\mathbb{F}_q$-subspace $\Rightarrow$ $dim_{\mathbb{F}_q} U \leq \frac{rn}{2}$

Maximum Scattered Spaces

Blokhuis-Lavrauw 2000

- $U \subset \mathbb{V} = V(r, q^n)$ scattered $\mathbb{F}_q$-subspace $\Rightarrow$ $dim_{\mathbb{F}_q} U \leq \frac{rn}{2}$
- $U \subset \mathbb{V} = V(r, q^n)$ scattered $\mathbb{F}_q$-subspace, $dim_{\mathbb{F}_q} U = \frac{rn}{2}$

$$\Downarrow$$

Maximum Scattered Spaces

Blokhuis-Lavrauw 2000

- $U \subset \mathbb{V} = V(r, q^n)$ scattered $\mathbb{F}_q$-subspace $\Rightarrow$ $dim_{\mathbb{F}_q} U \leq \frac{rn}{2}$
- $U \subset \mathbb{V} = V(r, q^n)$ scattered $\mathbb{F}_q$-subspace, $dim_{\mathbb{F}_q} U = \frac{rn}{2}$

$$\Downarrow$$

L_U is a two-intersection set (w.r.t. hyperplanes) in $PG(\mathbb{V}, \mathbb{F}_{q^n}) = PG(r-1, q^n)$.

Maximum Scattered Spaces

Blokhuis-Lavrauw 2000

- $U \subset \mathbb{V} = V(r, q^n)$ scattered $\mathbb{F}_q$-subspace $\Rightarrow$ $dim_{\mathbb{F}_q} U \leq \frac{rn}{2}$
- $U \subset \mathbb{V} = V(r, q^n)$ scattered $\mathbb{F}_q$-subspace, $dim_{\mathbb{F}_q} U = \frac{rn}{2}$

$$\Downarrow$$

L_U is a two-intersection set (w.r.t. hyperplanes) in $PG(\mathbb{V}, \mathbb{F}_{q^n}) = PG(r-1, q^n)$.

Two-weight linear codes

Two-weight linear codes $\longleftrightarrow$ Projective two-intersection sets

Maximum Scattered Spaces

Blokhuis-Lavrauw 2000

- $U \subset \mathbb{V} = V(r, q^n)$ scattered $\mathbb{F}_q$-subspace $\Rightarrow$ $dim_{\mathbb{F}_q} U \leq \frac{rn}{2}$
- $U \subset \mathbb{V} = V(r, q^n)$ scattered $\mathbb{F}_q$-subspace, $dim_{\mathbb{F}_q} U = \frac{rn}{2}$

$$\Downarrow$$

L_U is a two-intersection set (w.r.t. hyperplanes) in $PG(\mathbb{V}, \mathbb{F}_{q^n}) = PG(r-1, q^n)$.

Two-weight linear codes

Two-weight linear codes $\longleftrightarrow$ Projective two-intersection sets

Maximum Scattered Spaces

Blokhuis-Lavrauw 2000

- $U \subset \mathbb{V} = V(r, q^n)$ scattered $\mathbb{F}_q$-subspace $\Rightarrow$ $dim_{\mathbb{F}_q} U \leq \frac{rn}{2}$
- $U \subset \mathbb{V} = V(r, q^n)$ scattered $\mathbb{F}_q$-subspace, $dim_{\mathbb{F}_q} U = \frac{rn}{2}$

$$\Downarrow$$

L_U is a two-intersection set (w.r.t. hyperplanes) in $PG(\mathbb{V}, \mathbb{F}_{q^n}) = PG(r-1, q^n)$.

Two-weight linear codes

Two-weight linear codes $\longleftrightarrow$ Projective two-intersection sets

R. Calderbank, W.M. Kantor: The geometry of two-weight codes, *Bull. London Math. Soc.* (1986)

MRD-codes and Maximum Scattered Spaces

Sheekey, AMC (2016)

$$\mathcal{C} \in \mathcal{M}_L, \quad k = 2$$

$$\mathcal{C} \text{ MRD-code} \quad [n \times n, 2n, n-1]_{\mathbb{F}_q}, \quad L(\mathcal{C}) = \mathcal{F}_{q^n}$$

$$\mathcal{C} \simeq \mathcal{C}_f = [x, f(x)]_{\mathcal{F}_{q^n}}$$

$$\updownarrow$$

$$U_f = \{(x, f(x)) \, : \, x \in \mathbb{F}_{q^n}\} \subset \mathbb{V} = \mathbb{F}_{q^n} \times \mathbb{F}_{q^n}$$

Maximum Scattered $\mathbb{F}_q$-subspace of $\mathbb{V}$

MRD-codes and Maximum Scattered Spaces

Sheekey, AMC (2016)

$$\mathcal{C} \in \mathcal{M}_L, \quad k = 2$$

$\mathcal{C}$ MRD-code $\quad [n \times n, 2n, n-1]_{\mathbb{F}_q}, \quad L(\mathcal{C}) = \mathcal{F}_{q^n}$

$$\mathcal{C} \simeq \mathcal{C}_f = [x, f(x)]_{\mathcal{F}_{q^n}} \subset \mathcal{L}_{n,q} = V(n^2, q^n)$$

$$\updownarrow$$

$$U_f = \{(x, f(x)) \,:\, x \in \mathbb{F}_{q^n}\} \subset \mathbb{F}_{q^n} \times \mathbb{F}_{q^n} = V(2, q^n)$$

Maximum Scattered $\mathbb{F}_q$-subspace of $V(2, \mathbb{F}_{q^n})$

MRD-codes and Maximum Scattered Spaces

Sheekey, AMC (2016)

MRD-codes and Maximum Scattered Spaces

Sheekey, AMC (2016)

$$U_f \simeq U_g \text{ w.r.t. } \Gamma L(V(2,q^n)) \iff \mathcal{C}_f \simeq \mathcal{C}_g \text{ as MRD-codes}$$

MRD-codes and Maximum Scattered Spaces

Sheekey, AMC (2016)

$$U_f \simeq U_g \text{ w.r.t. } \Gamma L(V(2, q^n)) \iff \mathcal{C}_f \simeq \mathcal{C}_g \text{ as MRD-codes}$$

Known examples

MRD-codes and Maximum Scattered Spaces

Sheekey, AMC (2016)

$$U_f \simeq U_g \text{ w.r.t. } \Gamma L(V(2,q^n)) \iff \mathcal{C}_f \simeq \mathcal{C}_g \text{ as MRD-codes}$$

Known examples

- $U_1 = \{(x, x^{q^s}) \colon x \in \mathbb{F}_{q^n}\}$, $1 \leq s \leq n-1$, $\gcd(s,n) = 1$.
- $U_2 = \{(x, \delta x^{q^s} + x^{q^{n-s}}) \colon x \in \mathbb{F}_{q^n}\}$, $N_{q^n/q}(\delta) \neq 0, 1$, $\gcd(s,n) = 1$.

MRD-codes and Maximum Scattered Spaces

Sheekey, AMC (2016)

$$U_f \simeq U_g \text{ w.r.t. } \Gamma L(V(2,q^n)) \iff \mathcal{C}_f \simeq \mathcal{C}_g \text{ as MRD-codes}$$

Known examples

- $U_1 = \{(x, x^{q^s}) \colon x \in \mathbb{F}_{q^n}\}$, $1 \leq s \leq n-1$, $\gcd(s,n) = 1$.

  Blokhuis-Lavrauw: Scattered spaces with respect to a spread in *PG*(n,q), *Geom. Dedicata* (2000)

- $U_2 = \{(x, \delta x^{q^s} + x^{q^{n-s}}) \colon x \in \mathbb{F}_{q^n}\}$, $N_{q^n/q}(\delta) \neq 0, 1$, $\gcd(s,n) = 1$.

  Lunardon-O.P.: Blocking sets and derivable partial spreads, *J. Algebr. Comb.* (2001)

MRD-codes and maximum scattered spaces

Sheekey, AMC (2016)

$$U_f \simeq U_g \text{ w.r.t. } \Gamma L(V) \iff \mathcal{C}_f \simeq \mathcal{C}_g \text{ as MRD-codes}$$

Known examples

- $U_1 \quad \longleftrightarrow \quad \mathcal{C}_1 \in \mathcal{G}$

MRD-codes and maximum scattered spaces

Sheekey, AMC (2016)

$$U_f \simeq U_g \text{ w.r.t. } \Gamma L(V) \iff \mathcal{C}_f \simeq \mathcal{C}_g \text{ as MRD-codes}$$

Known examples

- $U_1 \longleftrightarrow \mathcal{C}_1 \in \mathcal{G}$
- $U_2 \longleftrightarrow \mathcal{C}_2 \in \mathcal{H}_L$

New examples

- $U_3 = \{(x, \delta x^{q^s} + x^{q^{s+n/2}}) \colon x \in \mathbb{F}_{q^n}\}$, $N_{q^n/q^{n/2}}(\delta) \notin \{0, 1\}$, $\gcd(s, n/2) = 1$,

New examples

- $U_3 = \{(x, \delta x^{q^s} + x^{q^{s+n/2}}) \colon x \in \mathbb{F}_{q^n}\}$, $N_{q^n/q^{n/2}}(\delta) \notin \{0, 1\}$, $\gcd(s, n/2) = 1$,

  Csajbók-Marino-O.P.-Zanella: A new family of MRD-codes, https://arxiv.org/abs/1707.08487 (2017)

New examples

- $U_3 = \{(x, \delta x^{q^s} + x^{q^{s+n/2}}) \colon x \in \mathbb{F}_{q^n}\}$, $N_{q^n/q^{n/2}}(\delta) \notin \{0, 1\}$, $\gcd(s, n/2) = 1$, $n = 6$ and $q > 4$, $n = 8$ and q odd

  Csajbók-Marino-O.P.-Zanella: A new family of MRD-codes, https://arxiv.org/abs/1707.08487 (2017)

New examples

- $U_3 = \{(x, \delta x^{q^s} + x^{q^{s+n/2}}) \colon x \in \mathbb{F}_{q^n}\}$, $N_{q^n/q^{n/2}}(\delta) \notin \{0,1\}$, $\gcd(s, n/2) = 1$, $n = 6$ and $q > 4$, $n = 8$ and q odd

  Csajbók-Marino-O.P.-Zanella: A new family of MRD-codes, https://arxiv.org/abs/1707.08487 (2017)

- $U_4 = \{(x, x^q + x^{q^3} + \delta x^{q^5}) \colon x \in \mathbb{F}_{q^6}\}$, with $\delta^2 + \delta = 1$, $q \equiv 0, \pm 1 \pmod 5$

New examples

- $U_3 = \{(x, \delta x^{q^s} + x^{q^{s+n/2}}) \colon x \in \mathbb{F}_{q^n}\}$, $N_{q^n/q^{n/2}}(\delta) \notin \{0,1\}$, $\gcd(s, n/2) = 1$, $n = 6$ and $q > 4$, $n = 8$ and q odd

  Csajbók-Marino-O.P.-Zanella: A new family of MRD-codes, https://arxiv.org/abs/1707.08487 (2017)

- $U_4 = \{(x, x^q + x^{q^3} + \delta x^{q^5}) \colon x \in \mathbb{F}_{q^6}\}$, with $\delta^2 + \delta = 1$, $q \equiv 0, \pm 1 \pmod 5$

  Csajbók-Marino-Zullo: New scattered linear sets of the projective line, ArXiv (2017)

New examples

- $U_3 = \{(x, \delta x^{q^s} + x^{q^{s+n/2}}) : x \in \mathbb{F}_{q^n}\}$, $N_{q^n/q^{n/2}}(\delta) \notin \{0, 1\}$, $\gcd(s, n/2) = 1$, $n = 6$ and $q > 4$, $n = 8$ and q odd

  Csajbók-Marino-O.P.-Zanella: A new family of MRD-codes, https://arxiv.org/abs/1707.08487 (2017)

- $U_4 = \{(x, x^q + x^{q^3} + \delta x^{q^5}) : x \in \mathbb{F}_{q^6}\}$, with $\delta^2 + \delta = 1$, $q \equiv 0, \pm 1 \pmod 5$

  Csajbók-Marino-Zullo: New scattered linear sets of the projective line, ArXiv (2017)

$$k = 2, n = 6, 8 \quad \Rightarrow \quad \mathcal{H}_L \subset \mathcal{M}_L$$

MRD-codes and Maximum Scattered Spaces

Classification results

- $\mathcal{C}$ MRD-code, $[3 \times 3, 6, 2]_{\mathbb{F}_q}$, $\mathbb{F}_{q^3}$-linear

MRD-codes and Maximum Scattered Spaces

Classification results

- $\mathcal{C}$ MRD-code, $[3 \times 3, 6, 2]_{\mathbb{F}_q}$, $\mathbb{F}_{q^3}$-linear

$$\mathcal{C} \in \mathcal{G}$$

MRD-codes and Maximum Scattered Spaces

Classification results

- $\mathcal{C}$ MRD-code, $[3 \times 3, 6, 2]_{\mathbb{F}_q}$, $\mathbb{F}_{q^3}$-linear

$$\mathcal{C} \in \mathcal{G}$$

Lavrauw-Van De Voorde: On linear sets on a projective line, *Des. Codes Cryptogr.* (2010)

MRD-codes and Maximum Scattered Spaces

Classification results

- $\mathcal{C}$ MRD-code, $[3 \times 3, 6, 2]_{\mathbb{F}_q}$, $\mathbb{F}_{q^3}$-linear

$$\mathcal{C} \in \mathcal{G}$$

Lavrauw-Van De Voorde: On linear sets on a projective line, *Des. Codes Cryptogr.* (2010)

- $\mathcal{C}$ MRD-code, $[4 \times 4, 8, 3]_{\mathbb{F}_q}$, $\mathbb{F}_{q^4}$-linear

MRD-codes and Maximum Scattered Spaces

Classification results

- $\mathcal{C}$ MRD-code, $[3 \times 3, 6, 2]_{\mathbb{F}_q}$, $\mathbb{F}_{q^3}$-linear

$$\mathcal{C} \in \mathcal{G}$$

Lavrauw-Van De Voorde: On linear sets on a projective line, *Des. Codes Cryptogr.* (2010)

- $\mathcal{C}$ MRD-code, $[4 \times 4, 8, 3]_{\mathbb{F}_q}$, $\mathbb{F}_{q^4}$-linear

$$\mathcal{C} \in \mathcal{G} \qquad \mathcal{C} \in \mathcal{H}_L$$

MRD-codes and Maximum Scattered Spaces

Classification results

- $\mathcal{C}$ MRD-code, $[3 \times 3, 6, 2]_{\mathbb{F}_q}$, $\mathbb{F}_{q^3}$-linear

  $$\mathcal{C} \in \mathcal{G}$$

  Lavrauw-Van De Voorde: On linear sets on a projective line, *Des. Codes Cryptogr.* (2010)

- $\mathcal{C}$ MRD-code, $[4 \times 4, 8, 3]_{\mathbb{F}_q}$, $\mathbb{F}_{q^4}$-linear

  $$\mathcal{C} \in \mathcal{G} \qquad \mathcal{C} \in \mathcal{H}_L$$

  Bonoli-O.P.: $\mathbb{F}_q$-linear blocking sets in $PG(2, q^4)$, *Innovations in Incidence Geometry* (2005)

MRD-codes and Maximum Scattered Spaces

Classification results

- $\mathcal{C}$ MRD-code, $[3 \times 3, 6, 2]_{\mathbb{F}_q}$, $\mathbb{F}_{q^3}$-linear

$$\mathcal{C} \in \mathcal{G}$$

Lavrauw-Van De Voorde: On linear sets on a projective line, *Des. Codes Cryptogr.* (2010)

- $\mathcal{C}$ MRD-code, $[4 \times 4, 8, 3]_{\mathbb{F}_q}$, $\mathbb{F}_{q^4}$-linear

$$\mathcal{C} \in \mathcal{G} \qquad \mathcal{C} \in \mathcal{H}_L$$

Bonoli-O.P.: $\mathbb{F}_q$-linear blocking sets in $PG(2, q^4)$, *Innovations in Incidence Geometry* (2005)
Csajbók-Zanella: Maximum scattered linear sets of $PG(1, q^4)$, *Discrete Mathematics* (2017)

MRD-codes and Maximum Scattered Spaces

Classification results

- $\mathcal{C}$ MRD-code, $[3 \times 3, 6, 2]_{\mathbb{F}_q}$, $\mathbb{F}_{q^3}$-linear

$$\mathcal{C} \in \mathcal{G}$$

  Lavrauw-Van De Voorde: On linear sets on a projective line, *Des. Codes Cryptogr.* (2010)

- $\mathcal{C}$ MRD-code, $[4 \times 4, 8, 3]_{\mathbb{F}_q}$, $\mathbb{F}_{q^4}$-linear

$$\mathcal{C} \in \mathcal{G} \qquad \mathcal{C} \in \mathcal{H}_L$$

  Bonoli-O.P.: $\mathbb{F}_q$-linear blocking sets in $PG(2, q^4)$, *Innovations in Incidence Geometry* (2005)
  Csajbók-Zanella: Maximum scattered linear sets of $PG(1, q^4)$, *Discrete Mathematics* (2017)
  For $q = 2$- **Horlemann-Trautmann, Marshall**: New criteria for MRD and Gabidulin codes and some rank-metric code constructions,arXiv:1507.08641v3 (2015)

MRD-codes and the Segre Variety

Lunardon, JCTA (2017)

$$End(\mathbb{F}_{q^n}, \mathbb{F}_q) = V(n^2, q) \quad \longrightarrow \quad \mathbb{P} = PG(n^2 - 1, q)$$

MRD-codes and the Segre Variety

Lunardon, JCTA (2017)

$$End(\mathbb{F}_{q^n}, \mathbb{F}_q) = V(n^2, q) \quad \longrightarrow \quad \mathbb{P} = PG(n^2-1, q)$$

$$\text{rank 1 linear maps} \quad \longrightarrow \quad \mathcal{S}_{n,n} \subset \mathbb{P} = PG(n^2-1, q)$$

MRD-codes and the Segre Variety

Lunardon, JCTA (2017)

$$End(\mathbb{F}_{q^n}, \mathbb{F}_q) = V(n^2, q) \quad \longrightarrow \quad \mathbb{P} = PG(n^2 - 1, q)$$

$$\text{rank 1 linear maps} \quad \longrightarrow \quad \mathcal{S}_{n,n} \subset \mathbb{P} = PG(n^2 - 1, q)$$

$$\text{rank} \leq h \text{ linear maps} \quad \longrightarrow \quad \mathcal{S}^h_{n,n} \subset \mathbb{P} = PG(n^2 - 1, q)$$

MRD-codes and the Segre Variety

Lunardon, JCTA (2017)

$$End(\mathbb{F}_{q^n}, \mathbb{F}_q) = V(n^2, q) \quad \longrightarrow \quad \mathbb{P} = PG(n^2 - 1, q)$$

$$\text{rank 1 linear maps} \quad \longrightarrow \quad \mathcal{S}_{n,n} \subset \mathbb{P} = PG(n^2 - 1, q)$$

$$\text{rank} \leq h \text{ linear maps} \quad \longrightarrow \quad \mathcal{S}^h_{n,n} \subset \mathbb{P} = PG(n^2 - 1, q)$$

$\mathcal{C} \subset End(\mathbb{F}_{q^n}, \mathbb{F}_q)$ linear MRD-code, $\quad [n \times n, kn, n - k + 1]_{\mathbb{F}_q}$

MRD-codes and the Segre Variety

Lunardon, JCTA (2017)

$$End(\mathbb{F}_{q^n}, \mathbb{F}_q) = V(n^2, q) \quad \longrightarrow \quad \mathbb{P} = PG(n^2-1, q)$$

$$\text{rank 1 linear maps} \quad \longrightarrow \quad \mathcal{S}_{n,n} \subset \mathbb{P} = PG(n^2-1, q)$$

$$\text{rank} \leq h \text{ linear maps} \quad \longrightarrow \quad \mathcal{S}^h_{n,n} \subset \mathbb{P} = PG(n^2-1, q)$$

$\mathcal{C} \subset End(\mathbb{F}_{q^n}, \mathbb{F}_q)$ linear MRD-code, $\quad [n \times n, kn, n-k+1]_{\mathbb{F}_q}$

$$\updownarrow$$

MRD-codes and the Segre Variety

Lunardon, JCTA (2017)

$$End(\mathbb{F}_{q^n}, \mathbb{F}_q) = V(n^2, q) \quad \longrightarrow \quad \mathbb{P} = PG(n^2-1, q)$$

$$\text{rank 1 linear maps} \quad \longrightarrow \quad \mathcal{S}_{n,n} \subset \mathbb{P} = PG(n^2-1, q)$$

$$\text{rank} \leq h \text{ linear maps} \quad \longrightarrow \quad \mathcal{S}^h_{n,n} \subset \mathbb{P} = PG(n^2-1, q)$$

$\mathcal{C} \subset End(\mathbb{F}_{q^n}, \mathbb{F}_q)$ linear MRD-code, $\quad [n \times n, kn, n-k+1]_{\mathbb{F}_q}$

$$\updownarrow$$

$P(\mathcal{C}) \subset \mathbb{P} \quad dim\, P(\mathcal{C}) = nk - 1$ such that

MRD-codes and the Segre Variety

Lunardon, JCTA (2017)

$$End(\mathbb{F}_{q^n}, \mathbb{F}_q) = V(n^2, q) \quad \longrightarrow \quad \mathbb{P} = PG(n^2-1, q)$$

$$\text{rank 1 linear maps} \quad \longrightarrow \quad \mathcal{S}_{n,n} \subset \mathbb{P} = PG(n^2-1, q)$$

$$\text{rank} \leq h \text{ linear maps} \quad \longrightarrow \quad \mathcal{S}^h_{n,n} \subset \mathbb{P} = PG(n^2-1, q)$$

$\mathcal{C} \subset End(\mathbb{F}_{q^n}, \mathbb{F}_q)$ linear MRD-code, $\quad [n \times n, kn, n-k+1]_{\mathbb{F}_q}$

$$\updownarrow$$

$P(\mathcal{C}) \subset \mathbb{P} \quad dim\, P(\mathcal{C}) = nk - 1$ such that

$$P(\mathcal{C}) \cap \mathcal{S}^{n-k}_{n,n} = \emptyset$$

MRD-codes and the Segre Variety

Lunardon, JCTA (2017)

$$End(\mathbb{F}_{q^n}, \mathbb{F}_q) = V(n^2, q) \quad \longrightarrow \quad \mathbb{P} = PG(n^2-1, q)$$

$$\text{rank 1 linear maps} \quad \longrightarrow \quad \mathcal{S}_{n,n} \subset \mathbb{P} = PG(n^2-1, q)$$

$$\text{rank} \leq h \text{ linear maps} \quad \longrightarrow \quad \mathcal{S}^h_{n,n} \subset \mathbb{P} = PG(n^2-1, q)$$

$\mathcal{C} \subset End(\mathbb{F}_{q^n}, \mathbb{F}_q)$ linear MRD-code, $\quad [n \times n, kn, n-k+1]_{\mathbb{F}_q}$

$$\updownarrow$$

$$P(\mathcal{C}) \quad \Rightarrow \quad P(\mathcal{C})^{\Phi} = P(\mathcal{C}^T)$$

MRD-codes and the Segre Variety

Lunardon, JCTA (2017)

$$End(\mathbb{F}_{q^n}, \mathbb{F}_q) = V(n^2, q) \quad \longrightarrow \quad \mathbb{P} = PG(n^2-1, q)$$

$$\text{rank 1 linear maps} \quad \longrightarrow \quad \mathcal{S}_{n,n} \subset \mathbb{P} = PG(n^2-1, q)$$

$$\text{rank} \leq h \text{ linear maps} \quad \longrightarrow \quad \mathcal{S}^h_{n,n} \subset \mathbb{P} = PG(n^2-1, q)$$

$\mathcal{C} \subset End(\mathbb{F}_{q^n}, \mathbb{F}_q)$ linear MRD-code, $\quad [n \times n, kn, n-k+1]_{\mathbb{F}_q}$

$$\updownarrow$$

$$P(\mathcal{C}) \quad \Rightarrow \quad P(\mathcal{C})^{\Phi} = P(\mathcal{C}^T)$$

$$P(\mathcal{C}) \quad \Rightarrow \quad P(\mathcal{C})^{\tau} = P(\mathcal{C}^{\perp})$$

Open problems

Open problems

Open problems

Open problems

- Understand whether $\mathcal{G} = \mathcal{M}_{L,R}$

Open problems

Open problems

- Understand whether $\mathcal{G} = \mathcal{M}_{L,R}$

$$k = 1,\ k = n - 1$$

$$k = 2,\ k = n - 2$$

Open problems

Open problems

- Understand whether $\mathcal{G} = \mathcal{M}_{L,R}$
$$k = 1,\ k = n-1$$
$$k = 2,\ k = n-2$$
- Find new examples in the family $\mathcal{M}_L \setminus \mathcal{H}_L$ existing for an infinite number of values of q and n.

Open problems

Open problems

- Understand whether $\mathcal{G} = \mathcal{M}_{L,R}$

$$k = 1,\ k = n - 1$$

$$k = 2,\ k = n - 2$$

- Find new examples in the family $\mathcal{M}_L \setminus \mathcal{H}_L$ existing for an infinite number of values of q and n.
- Generalize the connection found by Sheekey between linear sets and MRD-codes for the whole family $\mathcal{M}_L$.

Open problems

Open problems

- Understand whether $\mathcal{G} = \mathcal{M}_{L,R}$
$$k = 1, k = n - 1$$
$$k = 2, k = n - 2$$
- Find new examples in the family $\mathcal{M}_L \setminus \mathcal{H}_L$ existing for an infinite number of values of q and n.
- Generalize the connection found by Sheekey between linear sets and MRD-codes for the whole family $\mathcal{M}_L$.
- Understand the relationship between Sheekey's construction and Lunardon's approach.

Thank you

Thank you!