New scattered sequences of order $m \geq 3$

joint work with Giuseppe Marino

Alessandro Giannoni University Federico II of Naples
Perugia-WCC 2024 June 20, 2024

Connection

- Finite Field constructions: designs, blocking sets, translation planes...

Connection

- Finite Field constructions: designs, blocking sets, translation planes...

- MRD Codes: Random network coding

[1] D. Silva, F. R. Kschischang and R. Kötter, *A rank-metric approach to error control in random network coding*, IEEE Trans. Inform. Theory, Volume 54, 2008

Outline

1. Introduction
2. Scattered polynomials and sequences
3. Main result
4. Generalization with h-scattered sequences
5. Future perspective

Introduction

Setting

- q is a prime power, n, m, k are positive integers
- $\mathbb{F}_q$, $\mathbb{F}_{q^n}$
- $\mathbb{F}_{q^n}[X], \mathbb{F}_{q^n}[X_1, \ldots, X_m]$

$\mathbb{F}_q$-subsspaces

Definition

$U \subset \mathbb{F}_{q^n}^k$ is said to be an $\mathbb{F}_q$-subspace if:

- $u_1 + u_2 \in U$ for every $u_1, u_2 \in U$
- $\lambda u_1 \in U$ for every $u_1 \in U, \lambda \in \mathbb{F}_q$.

q-linearized polynomials

Definition

$f \in \mathbb{F}_{q^n}[X]$ is said to be q-linearized if:

- $f(x+y) = f(x) + f(y)$ for every $x, y \in \mathbb{F}_{q^n}$ (f is additive)
- $f(\lambda x) = \lambda f(x)$ for every $x \in \mathbb{F}_{q^n}, \lambda \in \mathbb{F}_q$.

q-linearized polynomials

$$L_{n,q}[X] := \left\{ \sum_{i=0}^{\ell} a_i X^{q^i} : a_i \in \mathbb{F}_{q^n}, \ell \in \mathbb{N}^+ \right\}$$

q-linearized polynomials

$$\mathcal{L}_{n,q}[X] := L_{n,q}[X]/(X^{q^n} - X) = \{\sum_{i=0}^{n-1} a_i X^{q^i} : a_i \in \mathbb{F}_{q^n}\}$$

q-linearized polynomials

$$\mathcal{L}_{n,q}[X_1, \dots, X_m] := \mathcal{L}_{n,q}[X_1] \oplus \cdots \oplus \mathcal{L}_{n,q}[X_m]$$

h-scattered $\mathbb{F}_q$-subspaces

Definition

Let $h, t \in \mathbb{N}$, such that $h < k$ and $h \leq t$. An $\mathbb{F}_q$-subspace $U \subseteq \mathbb{F}_{q^n}^k$ is said to be (h, t)-evasive if for every h-dimensional $\mathbb{F}_{q^n}$-subspace $H \subseteq \mathbb{F}_{q^n}^k$, it holds $\dim_{\mathbb{F}_q}(U \cap H) \leq t$. When $h = t$, an (h, h)-evasive subspace is called h-scattered.

Maximum h-scattered $\mathbb{F}_q$-subspaces

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

If U is an h-scattered subspace in $\mathbb{F}_{q^n}^k$ that does not define a subgeometry, then

$$\dim_{\mathbb{F}_q}(U) \leq \frac{nk}{h+1}.$$

Scattered polynomials and sequences

Construction of scattered subspaces

Let $f \in \mathcal{L}_{n,q}[X]$, we can consider

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

Construction of *h*-scattered subspaces

Let $\mathcal{F} = (f_1, \dots, f_s)$, with $f_1, \dots, f_s \in \mathcal{L}_{n,q}[X_1, \dots, X_m]$

$$U_{\mathcal{F}} = \{(x_1, \dots, x_m, f_1(\underline{x}), \dots, f_s(\underline{x})) \, : \, x_1, \dots, x_m \in \mathbb{F}_{q^n}\}$$

where $\underline{x} = (x_1, \dots, x_m)$.

Construction of h-scattered subspaces

- $\mathcal{F}$ scattered $\longrightarrow nm = \dim_{\mathbb{F}_q}(U_{\mathcal{F}}) \stackrel{?}{=} \frac{n(m+s)}{2} \longrightarrow s = m$

Construction of *h*-scattered subspaces

- $\mathcal{F}$ scattered $\longrightarrow nm = \dim_{\mathbb{F}_q}(U_{\mathcal{F}}) \overset{?}{=} \frac{n(m+s)}{2} \longrightarrow s = m$

- $\mathcal{F}$ h-scattered $\longrightarrow nm = \dim_{\mathbb{F}_q}(U_{\mathcal{F}}) \overset{?}{=} \frac{n(m+s)}{h+1} \longrightarrow s = hm$

Indecomposability

$$\mathcal{F} \overset{?}{\simeq} (\mathcal{G}_1, \mathcal{G}_2)$$

where $\mathcal{G}_1 = (g_1^{(1)}, \dots, g_{s_1}^{(1)})$, $\mathcal{G}_2 = (g_1^{(2)}, \dots, g_{s_2}^{(2)})$ and $\mathcal{F} = (f_1, \dots, f_{s_1+s_2})$, with $g_i^{(1)}, g_i^{(2)}, f_i \in \mathcal{L}_{n,q}[X_1, \dots, X_m]$.

$h = 1$

- $m = 1$: Scattered Polynomials, $\{(x, f(x)) : x \in \mathbb{F}_{q^n}\}$

$h = 1$

- $m = 1$: Scattered Polynomials, $\{(x, f(x)) : x \in \mathbb{F}_{q^n}\}$
- $m = 2$: $\left\{\left(x, y, x^{q^I} + \alpha y^{q^J}, x^{q^J} + \beta y^{q^I} + \gamma y^{q^J}\right) \ : \ x, y \in \mathbb{F}_{q^n}\right\}$

[2] D. Bartoli and G. Marino and A. Neri and L. Vicino, *Exceptional scattered sequences*, (2024)

Main result

Setting

Let $m > 2$, $J, I \in \mathbb{N}$, $J > I$, $\mathbf{A} = (\alpha_1, \ldots, \alpha_m)$ with $\alpha_1, \ldots, \alpha_m \in \mathbb{F}_{q^n}$.

Setting

Let $m > 2$, $J, I \in \mathbb{N}$, $J > I$, $\mathbf{A} = (\alpha_1, \dots, \alpha_m)$ with $\alpha_1, \dots, \alpha_m \in \mathbb{F}_{q^n}$.

$$
\begin{aligned}
f_1(x_1, \dots, x_m) &:= x_1{}^{q^I} + \alpha_2 x_2{}^{q^J} \\
f_2(x_1, \dots, x_m) &:= x_2{}^{q^I} + \alpha_3 x_3{}^{q^J} \\
&\vdots \\
f_{m-1}(x_1, \dots, x_m) &:= x_{m-1}{}^{q^I} + \alpha_m x_m{}^{q^J} \\
f_m(x_1, \dots, x_m) &:= x_m{}^{q^I} + \alpha_1 x_1{}^{q^J}.
\end{aligned}
$$

Setting

Let $m > 2$, $J, I \in \mathbb{N}$, $J > I$, $\mathbf{A} = (\alpha_1, \dots, \alpha_m)$ with $\alpha_1, \dots, \alpha_m \in \mathbb{F}_{q^n}$.

$$
\begin{aligned}
f_1(x_1, \dots, x_m) &:= x_1^{q^I} + \alpha_2 x_2^{q^J} \\
f_2(x_1, \dots, x_m) &:= x_2^{q^I} + \alpha_3 x_3^{q^J} \\
&\vdots \\
f_{m-1}(x_1, \dots, x_m) &:= x_{m-1}^{q^I} + \alpha_m x_m^{q^J} \\
f_m(x_1, \dots, x_m) &:= x_m^{q^I} + \alpha_1 x_1^{q^J}.
\end{aligned}
$$

Let $\mathcal{F}_{\mathbf{A}} := (f_1, \dots, f_m)$.

Setting

$$U_{\mathbf{A}}^{I,J} := U_{\mathcal{F}_{\mathbf{A}}} = \{(x_1, \ldots, x_m, f_1(\underline{x}), f_2(\underline{x}), \ldots, f_{m-1}(\underline{x}), f_m(\underline{x})) : \underline{x} \in (\mathbb{F}_{q^n})^m\},$$

Setting

- $\mathbf{K} := J - I$
- $K_{\mathbf{A}}^{I,J} := \frac{\alpha_3 \cdot \alpha_4^{q^{\mathbf{K}}} \cdot \alpha_5^{q^{2\mathbf{K}}} \ldots \alpha_m^{q^{(m-3)\mathbf{K}}} \cdot \alpha_1^{q^{(m-2)\mathbf{K}}}}{\alpha_2^{1+q^{\mathbf{K}}+\cdots+q^{(m-2)\mathbf{K}}}}$
- $C_{\mathbf{K},m} := \frac{q^{m\mathbf{K}}-1}{q^{\mathbf{K}}-1}$

Properties of $U_{\mathbf{A}}^{I,J}$

Theorem (Bartoli, A.G., Marino, 202x)

If $(I,J)=1$, then $U_{\mathbf{A}}^{I,J}$ is maximum scattered for any $\mathbf{A} \in \Omega$,

where

$$\Omega := \{\mathbf{A} = (\alpha_1, \ldots, \alpha_m) : K_{\mathbf{A}}^{I,J} \text{ is not a } C_{\mathbf{K},m}\text{-power in } \mathbb{F}_{q^n}\}.$$

Properties of $U_{\mathbf{A}}^{I,J}$

Remark

$C_{a,b} := \frac{q^{ab}-1}{q^{a}-1}$

Proposition

Let $B \in \mathbb{N}$ such that $(q, B) = 1$, then there exist infinitely many $\ell_k \in \mathbb{N}$ such that $(B, C_{n,\ell_k}) = 1$.

Properties of $U_{\mathbf{A}}^{I,J}$

Remark

$C_{a,b} := \frac{q^{ab}-1}{q^{a}-1}$

Proposition

Let $B \in \mathbb{N}$ such that $(q, B) = 1$, then there exist infinitely many $\ell_k \in \mathbb{N}$ such that $(B, C_{n,\ell_k}) = 1$.

Observation

Let $(\ell_k)_{k>0}$ be the numerical sequence obtained by the previous proposition then given $x \in \mathbb{F}_{q^n}$ such that is not a B-power in $\mathbb{F}_{q^n}$ then x is not a B-power in $\mathbb{F}_{q^{n\ell_k}}$ for every $k > 0$.

Properties of $U_{\mathbf{A}}^{I,J}$

$K_{\mathbf{A}}^{I,J}$ is not a $C_{\mathbf{K},m}$-power in $\mathbb{F}_{q^n}$

Properties of $U_{\mathbf{A}}^{I,J}$

$$K_{\mathbf{A}}^{I,J} \text{ is not a } C_{\mathbf{K},m}\text{-power in } \mathbb{F}_{q^n}$$

$$\downarrow$$

$$K_{\mathbf{A}}^{I,J} \text{ is not a } C_{\mathbf{K},m}\text{-power in } \mathbb{F}_{q^{n\ell_k}} \text{ for every } k > 0$$

Properties of $U_{\mathbf{A}}^{I,J}$

$$K_{\mathbf{A}}^{I,J} \text{ is not a } C_{\mathbf{K},m}\text{-power in } \mathbb{F}_{q^n}$$

$$\downarrow$$

$$K_{\mathbf{A}}^{I,J} \text{ is not a } C_{\mathbf{K},m}\text{-power in } \mathbb{F}_{q^{n\ell_k}} \text{ for every } k > 0$$

$$\downarrow \text{(Using the first Theorem)}$$

$$\mathcal{F}_{\mathbf{A}} \text{ is scattered in } \mathbb{F}_{q^{n\ell_k}} \text{ for every } k > 0$$

Properties of $U_{\mathbf{A}}^{I,J}$

$$K_{\mathbf{A}}^{I,J} \text{ is not a } C_{\mathbf{K},m}\text{-power in } \mathbb{F}_{q^n}$$

$$\downarrow$$

$$K_{\mathbf{A}}^{I,J} \text{ is not a } C_{\mathbf{K},m}\text{-power in } \mathbb{F}_{q^{n\ell_k}} \text{ for every } k > 0$$

$$\downarrow \text{ (Using the first Theorem)}$$

$$\mathcal{F}_{\mathbf{A}} \text{ is scattered in } \mathbb{F}_{q^{n\ell_k}} \text{ for every } k > 0$$

$$\downarrow$$

$$\mathcal{F}_{\mathbf{A}} \text{ is exceptional scattered}$$

Properties of $U_{\mathbf{A}}^{I,J}$

Lemma (Bartoli, Marino, Neri, Vicino)

Let $\mathcal{F} := (f_1, \ldots, f_s)$ be an exceptional h-scattered sequence of order m. If $U_{\mathcal{F}}$ is $(t, tn/(h+1)-1)$-evasive for any $t \in [h+1, \lfloor (m+s)/2 \rfloor]$ with $(h+1) \mid tn$, then $\mathcal{F}$ is indecomposable.

[2] D. Bartoli and G. Marino and A. Neri and L. Vicino, *Exceptional scattered sequences*, (2024)

Properties of $U_{\mathbf{A}}^{I,J}$

Lemma

Let $\mathcal{F} := (f_1, \ldots, f_m)$ be an exceptional scattered sequence of order m. If $U_{\mathcal{F}}$ is $(t, \frac{tn}{2} - 1)$-evasive for any $t \in [2, m]$ with tn even, then $\mathcal{F}$ is indecomposable.

Properties of $U_{\mathbf{A}}^{I,J}$

Theorem (Bartoli, A.G., Marino, 202x)

If $n \geq 2(mJ + J + 1)$ then $U_{\mathbf{A}}^{I,J}$ is $(t, \frac{tn}{2} - 1)$-evasive for any odd $t \in [2, \ldots, m]$ and $\mathbf{A} \in \Omega$.

Properties of $U_{\mathbf{A}}^{I,J}$

$$\Pi_i = \alpha_i^{q^{(m-1)\mathbf{K}}} \cdot \alpha_{i-1}^{q^{(m-2)\mathbf{K}}} \cdots \alpha_{i+2}^{q^{\mathbf{K}}} \cdot \alpha_{i+1} \quad \text{with } i = 1, \ldots, m$$

Properties of $U_{\mathbf{A}}^{I,J}$

$$\Pi_i = \alpha_i^{q^{(m-1)\mathbf{K}}} \cdot \alpha_{i-1}^{q^{(m-2)\mathbf{K}}} \cdots \alpha_{i+2}^{q^{\mathbf{K}}} \cdot \alpha_{i+1} \quad \text{with } i = 1, \dots, m$$

$$\Omega' := \left\{ \mathbf{A} \in \Omega \mid \frac{\Pi_{\delta+2}}{\Pi_2} \text{ is not a } (q^{m\mathbf{K}} - 1)\text{-power in } \mathbb{F}_{q^n}, \forall\, \delta = 1, \dots, m-1 \right\}$$

Properties of $U_{\mathbf{A}}^{I,J}$

Theorem (Bartoli, A.G., Marino, 202x)

If $n \geq 2(mJ + J + 1)$ then $U_{\mathbf{A}}^{I,J}$ is $(t, \frac{tn}{2} - 1)$-evasive for any even $t \in [2, \dots, m]$ and $\mathbf{A} \in \Omega'$.

Properties of $U_{\mathbf{A}}^{I,J}$

Theorem (Bartoli, A.G., Marino, 202x)
If $n \geq 2(mJ + J + 1)$ then $U_{\mathbf{A}}^{I,J}$ is indecomposable for any $\mathbf{A} \in \Omega'$.

Generalization with h-scattered sequences

Case $h>1$

Let $h > 1$, $\mathbf{A} = (\alpha_1, \ldots, \alpha_m) \in \mathbb{F}_{q^n}^m$

Case $h>1$

Let $h > 1$, **A** $= (\alpha_1, \dots, \alpha_m) \in \mathbb{F}_{q^n}^m$

$$\begin{aligned} f_{1,h}(x_1,\dots,x_m) &:= {x_1}^{q^h} + \alpha_2 {x_2}^{q^{h+1}} \\ f_{2,h}(x_1,\dots,x_m) &:= {x_2}^{q^h} + \alpha_3 {x_3}^{q^{h+1}} \\ &\vdots \\ f_{m-1,h}(x_1,\dots,x_m) &:= {x_{m-1}}^{q^h} + \alpha_m {x_m}^{q^{h+1}} \\ f_{m,h}(x_1,\dots,x_m) &:= {x_m}^{q^h} + \alpha_1 {x_1}^{q^{h+1}}. \end{aligned}$$

Let $\mathcal{F}_{\mathbf{A},h} := (f_{1,h}, \dots, f_{m,h})$.

Generalization

$$V_{\mathbf{A},h} := \{(\underline{x}, \underline{x}^q, \underline{x}^{q^2}, \ldots, \underline{x}^{q^{h-1}}, \mathcal{F}_{\mathbf{A},h}(\underline{x})) : \underline{x} \in (\mathbb{F}_{q^n})^m\} \subset \mathbb{F}_{q^n}^{(h+1)m}$$

where $\underline{x}^{q^j} = (x_1^{q^j}, \ldots, x_m^{q^j})$.

Generalization

Twisted Gabidulin

$$\{(x, x^q, x^{q^2}, \ldots, x^{q^{h-1}}, f(x)) \mid x \in \mathbb{F}_{q^n}\} \subset \mathbb{F}_{q^n}^{h+1}$$

$$\updownarrow$$

Vectorial Twisted Gabidulin

$$V_{\mathbf{A},h} = \{(\underline{x}, \underline{x}^q, \underline{x}^{q^2}, \ldots, \underline{x}^{q^{h-1}}, \mathcal{F}_{\mathbf{A},h}(\underline{x})) : \underline{x} \in (\mathbb{F}_{q^n})^m\} \subset \mathbb{F}_{q^n}^{(h+1)m}$$

Generalization

$$V_{\mathbf{A},h} = \{(\underline{x}, \mathcal{G}_{\mathbf{A},h}(\underline{x})) : \underline{x} \in (\mathbb{F}_{q^n})^m\} \subset \mathbb{F}_{q^n}^{(h+1)m}$$

$$\text{where } \mathcal{G}_{\mathbf{A},h} = (\underline{X}^q, \underline{X}^{q^2}, \ldots, \underline{X}^{q^{h-1}}, \mathcal{F}_{\mathbf{A},h})$$

Properties of $V_{\mathbf{A},h}$

Theorem (Bartoli, A.G., Marino, 202x)

$V_{\mathbf{A},h}$ is maximum h-scattered for every $\mathbf{A} \in \Omega$, $h > 1$.

Known subspaces

What are the known maximum h-scattered subspaces in $\mathbb{F}_{q^n}^{(h+1)m}$?

Known subspaces

What are the known maximum h-scattered subspaces in $\mathbb{F}_{q^n}^{(h+1)m}$?

$$G = \bigoplus_{i=1}^{m} G_i$$

where G_i is maximum h-scattered in $\mathbb{F}_{q^n}^{h+1}$ for every $i = 1, \dots, m$.

Comparison

j-th generalized weight in $\mathbb{F}_{q^n}^k$

$$d_j(U) = \dim_{\mathbb{F}_q}(U) - \max\{\dim_{\mathbb{F}_q}(H \cap U) \, : \, H \subseteq \mathbb{F}_{q^n}^k \text{ with } \dim_{\mathbb{F}_{q^n}}(H) = k - j\}$$

Comparison

- $d_{(m-1)(h+1)}(V_{\mathbf{A},h}) \geq mn - h - 2 \quad$ for every $\mathbf{A} \in \Omega$

  $d_{s(h+1)}(V_{\mathbf{A},h}) \geq (s+1)(n-h-1) \quad$ for every $s = 1, \ldots, m-2$, $\mathbf{A} \in \Omega'$

Comparison

- $d_{(m-1)(h+1)}(V_{\mathbf{A},h}) \geq mn - h - 2 \quad$ for every $\mathbf{A} \in \Omega$

  $d_{s(h+1)}(V_{\mathbf{A},h}) \geq (s+1)(n-h-1) \quad$ for every $s = 1, \ldots, m-2$, $\mathbf{A} \in \Omega'$

- $d_{s(h+1)}(G) \leq sn$ for every $s = 1, \ldots, m-1$

Comparison

Theorem (Bartoli, A.G., Marino, 202x)

The following hold.

- *If* $n > (s+1)(h+1)$*, then for any* $s = 1, \ldots, m-2$ *and for any* $\boldsymbol{A} \in \Omega'$

$$d_{s(h+1)}(V_{\mathbf{A},h}) > d_{s(h+1)}(G).$$

- *If* $n > h+2$*, then for any* $\boldsymbol{A} \in \Omega$

$$d_{(m-1)(h+1)}(V_{\mathbf{A},h}) > d_{(m-1)(h+1)}(G).$$

Comparison

Remark

$$\mathcal{G}_{\mathbf{A},h} = (\underline{X}^q, \underline{X}^{q^2}, \ldots, \underline{X}^{q^{h-1}}, \mathcal{F}_{\mathbf{A},h})$$

Proposition

If $\mathbf{A} \in \Omega'$ than there exist infinite positive integers $\{\ell_k\}_{k\in\mathbf{N}}$ such that $\mathcal{G}_{\mathbf{A},h}$ is h-scattered in $\mathbb{F}_{q^{n\ell_k}}$.

Future perspective

Future Perspectives

- Complete the study of the generalized weights

Future Perspectives

- Complete the study of the generalized weights
- Study this construction with different $\mathcal{F}$:

$$\{(\underline{x}, \underline{x}^q, \underline{x}^{q^2}, \ldots, \underline{x}^{q^{h-1}}, \mathcal{F}(\underline{x})) : \underline{x} \in (\mathbb{F}_{q^n})^m\}$$

THANK YOU FOR YOUR ATTENTION