Exceptional and indecomposable scattered sequences of order $m > 2$

(joint work with Daniele Bartoli and Giuseppe Marino)

Alessandro Giannoni

University Federico II of Napoli

OpeRa 2024 - Caserta

February 14, 2024

Summary

$\mathcal{F} = (f_1, \ldots, f_m)$ exceptional scattered, indecomposable and cutting

Summary

$\mathcal{F} = (f_1, \ldots, f_m)$ exceptional scattered, indecomposable and cutting

$$\downarrow$$

$\mathcal{C}_{\mathcal{F}}$ minimal and indecomposable MRD code

Summary

- Network coding
  - 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
- Cryptography
  - P. Loidreau, *A new rank metric codes based encryption scheme*, Post-quantum cryptography, Volume 10346 of *Lecture Notes in Comput. Sci.*, 2017 Pages 507-534

$\mathbb{F}_q$-subspaces

Let $q = p^h, n, k \in \mathbb{N}$.

Definition

$U \subset \mathbb{F}_{q^n}^k$ is said $\mathbb{F}_q$-subspace if it's closed under linear combination with coefficients in $\mathbb{F}_q$.

$\mathbb{F}_q$-subspaces

Let $q = p^h, n, k \in \mathbb{N}$.

Definition

$U \subset \mathbb{F}_{q^n}^k$ is said $\mathbb{F}_q$-subspace if it's closed under linear combination with coefficients in $\mathbb{F}_q$.

Definition

A $\mathbb{F}_q$-subspace U of dimension ℓ is said to be scattered if $|L(U)| = \frac{q^\ell - 1}{q-1}$.

$\mathbb{F}_q$-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.

q-linearized polynomials

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

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

q-linearized polynomials

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

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

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

q-linearized polynomials

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

D. Bartoli and Y. Zhou, *Exceptional scattered polynomials*, Journal of Algebra, Volume 509, 2018 Pages 507-534

q-linearized polynomials

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

D. Bartoli and Y. Zhou, *Exceptional scattered polynomials*, Journal of Algebra, Volume 509, 2018 Pages 507-534

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

D. Bartoli and G. Marino and A. Neri and L. Vicino, *Exceptional scattered sequences*, arXiv preprint arXiv:2211.11477 (2022)

Main results

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

Main results

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

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

Main results

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

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

Let $\mathcal{F} := (f_1, \ldots, f_m)$.

Main results

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

Main results

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

Main results

Theorem

If $\gcd(I, J) = 1$ *and* $K_{\mathbf{A}}^{I,J}$ *is not a* $C_{K,m}$*-power in* $\mathbb{F}_{q^n}$*,then* $U_{\mathbf{A}}^{I,J}$ *is maximum scattered.*

Main results

Proposition

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

Main results

Proposition

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

Observation

Let $(h_k)_{k>0}$ be the 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 $\mathbb{F}_{q^{nh_k}}$ for any $k > 0$.

Main results

Corollary

If $\gcd(I,J)=1$ *and* $K_{\mathbf{A}}^{I,J}$ *is not a* $C_{K,m}$*-power in* $\mathbb{F}_{q^n}$*,then* $U_{\mathbf{A}}^{I,J}$ *is exceptional scattered.*

Main results

Lemma

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.

D. Bartoli and G. Marino and A. Neri and L. Vicino, *Exceptional scattered sequences*, arXiv preprint arXiv:2211.11477 (2022)

Main results

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.

Main results

Theorem

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

Main results

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

Main results

Theorem

If $n \geq 2(mJ+J+1)$ *and* $\frac{\Pi_{\delta+2}}{\Pi_2}$ *is not a* $(q^{mK}-1)$*-power in* $\mathbb{F}_{q^n}$ *for any* $\delta = 1, \ldots, m-1$*, then* $U_{\mathbf{A}}^{I,J}$ *is* $(t, \frac{tn}{2}-1)$*-evasive for any even* $t \in [2, \ldots, m]$*.*

Main results

Theorem

If $n \geq 2(mJ+J+1)$ *and* $\frac{\Pi_{\delta+2}}{\Pi_2}$ *is not a* $(q^{mK}-1)$*-power in* $\mathbb{F}_{q^n}$ *for any* $\delta = 1, \ldots, m-1$, *then* $U_{\mathbf{A}}^{I,J}$ *is indecomposable.*

Main results

Observation

If $\frac{\Pi_{\delta+2}}{\Pi_2}$ *is not a* $(q^{mK}-1)$*-power in* $\mathbb{F}_{q^n}$ *for any* $\delta = 1, \ldots, m-1$ *then* $m|n$.

Main results

Theorem

Assume that $\gcd(I, J) = 1$, $K_{\mathbf{A}}^{I,J}$ *is not a* $C_{K,m}$*-power, and* $\frac{\Pi_{\delta+2}}{\Pi_2}$ *is not a* $(q^{mK} - 1)$*-power in* $\mathbb{F}_{q^n}$ *for any* $\delta = 1, \ldots, m-1$. *Then* $U_{\mathbf{A}}^{I,J}$ *is scattered and indecomposable in infinitely many extensions of* $\mathbb{F}_{q^n}$.

Proof Main result

By a previous Proposition there exists a sequence of positive integers $(h_k)_k$ such that $\gcd(q^{mK}-1, C_{n,h_k}) = 1$. This implies $\gcd(C_{K,m}, C_{n,h_k}) = 1$, so $K_{\mathbf{A}}^{I,J}$ is not a $C_{K,m}$-power in $\mathbb{F}_{q^{nh_k}}$ for any $k > 0$. So $U_{\mathbf{A}}^{I,J}$ is scattered in $\mathbb{F}_{q^{nh_k}}$ for any $k > 0$. Analogously we have that $\frac{\Pi_{\delta+2}}{\Pi_2}$ is not a $(q^{mK}-1)$-power in $\mathbb{F}_{q^{nh_k}}$ for any $k > 0$ and $\delta = 1, \ldots, m-1$.
Also, there exists an h_{k_0} such that

$$nh_{k_0} \geq 2(mJ + J + 1).$$

So we obtain that $U_{\mathbf{A}}^{I,J}$ is scattered and indecomposable in every extension $\mathbb{F}_{q^{nh_k}}$ with $h_k \geq h_{k_0}$.

□

Main results

Theorem

If $n \geq 2J+1$, *and there exists* $\delta \in [1, \ldots, m-1]$ *such that* $\frac{\Pi_{\delta+2}}{\Pi_2}$ *is not a* $(q^{mK}-1)$*-power in* $\mathbb{F}_{q^n}$, *then* $U_{\mathbf{A}}^{I,J}$ *is* $(2m-2, mn-n-1)$*-evasive.*

Main results

Theorem

Let U be an $[n, k]_{q^m/q}$ system. Then, U is $(k-2, n-m-1)$-evasive if and only if it is cutting.

D. Bartoli and G. Marino and A. Neri, *New MRD codes from linear cutting blocking sets*, Ann. Mat. Pura Appl. (1923-),Springer (2022)

Equivalence issue

Theorem

Let I, J, I_0, J_0 be nonnegative integers, such that $J + J_0 < n$, $I < J$, and $I_0 < J_0$. The two sets $U_{\mathbf{A}}^{I,J}$ and $U_{\mathbf{A_0}}^{I_0,J_0}$ are not $\Gamma L(2m, q^n)$-equivalent if $(I, J) \neq (I_0, J_0)$.

Equivalence issue

Theorem

Let (I, J) be such that $J < n/2$. Given $\mathbf{A} = (\alpha_1, \ldots, \alpha_m)$, $\mathbf{A_0} = (\beta_1, \ldots, \beta_m)$ then the sets $U^{I,J}_{\mathbf{A}}$ and $U^{I,J}_{\mathbf{A_0}}$ are $\Gamma L(2m, q^n)$-equivalent if and only if $\exists\, \sigma \in Aut(\mathbb{F}_{q^n})$ such that one among these m elements is a $q^{mK} - 1$ power:

$$C_1 := \left(\frac{\beta_2}{\alpha_2^\sigma}\right)\left(\frac{\beta_3}{\alpha_3^\sigma}\right)^{q^K} \cdots \left(\frac{\beta_m}{\alpha_m^\sigma}\right)^{q^{(m-2)K}} \left(\frac{\beta_1}{\alpha_1^\sigma}\right)^{q^{(m-1)K}}$$

$$C_\delta := \left(\frac{\beta_{\delta+1}}{\alpha_2^\sigma}\right) \cdots \left(\frac{\beta_m}{\alpha_{m-\delta+1}^\sigma}\right)^{q^{(m-\delta-1)K}} \left(\frac{\beta_1}{\alpha_{m-\delta+2}^\sigma}\right)^{q^{(m-\delta)K}} \cdots \left(\frac{\beta_\delta}{\alpha_1^\sigma}\right)^{q^{(m-1)K}}$$

$$C_m := \left(\frac{\beta_1}{\alpha_2^\sigma}\right) \cdots \left(\frac{\beta_{m-1}}{\alpha_m^\sigma}\right)^{q^{(m-2)K}} \left(\frac{\beta_m}{\alpha_1^\sigma}\right)^{q^{(m-1)K}},$$

with $\delta = 2, \ldots, m-1$.

Equivalence issue

$$\left(1-\frac{1}{\gcd(q^n-1,\frac{q^{mK}-1}{q^K-1})}-\sum_{j=1}^{\lceil\frac{m-1}{2}\rceil}\frac{q^{\gcd(mn',j)}-1}{q^{m\gcd(n',K)}-1}\right)\cdot\frac{q^{m\gcd(n',K)}-1}{mnh},$$

where $q=p^h, n=mn'$.

Future Perspectives

- Study of the automorphism group of $U_{\mathbf{A}}^{I,J}$;
- Change the binomials with trinomials
  $f_i = x_i^{q^I} + \alpha_{i+1}x_{i+1}^{q^J} + \beta_{i+2}x_{i+2}^{q^K}$

THANK YOU FOR YOUR ATTENTION