Sidon spaces and Cyclic Subspace Codes

Chiara Castello

Joint work with Olga Polverino, Paolo Santonastaso and Ferdinando Zullo

Università degli Studi della Campania “Luigi Vanvitelli”

Finite geometry and friends
A Brussels summer school on finite geometry
Vrije Universiteit Brussel

Subspace codes

R. Koetter, and F.R. Kschischang
Coding for errors and erasures in random network coding
IEEE Transaction on Information Theory, 2008.

Subspace codes

R. Koetter, and F.R. Kschischang
Coding for errors and erasures in random network coding
IEEE Transaction on Information Theory, 2008.

$U, V \in \mathcal{G}_q(n, m)$: the set of m-dimensional $\mathbb{F}_q$ subspaces of $\mathbb{F}_{q^n}$

Subspace codes

R. Koetter, and F.R. Kschischang
Coding for errors and erasures in random network coding
IEEE Transaction on Information Theory, 2008.

$U, V \in \mathcal{G}_q(n, m)$: the set of m-dimensional $\mathbb{F}_q$ subspaces of $\mathbb{F}_{q^n}$

$$d(U, V) := \dim_{\mathbb{F}_q}(U) + \dim_{\mathbb{F}_q}(V) - 2\dim_{\mathbb{F}_q}(U \cap V)$$

Subspace codes

R. Koetter, and F.R. Kschischang
Coding for errors and erasures in random network coding
IEEE Transaction on Information Theory, 2008.

$U, V \in \mathcal{G}_q(n, m)$: the set of m-dimensional $\mathbb{F}_q$ subspaces of $\mathbb{F}_{q^n}$

$$d(U, V) := \dim_{\mathbb{F}_q}(U) + \dim_{\mathbb{F}_q}(V) - 2\dim_{\mathbb{F}_q}(U \cap V)$$

$\mathcal{C} \subset \mathcal{G}_q(n, m)$, $(\mathcal{C}, d)$ *Constant dimension subspace code*

$$d(\mathcal{C}) := \min\{d(U, V) \,:\, U, V \in \mathcal{C}, U \neq V\}$$

minimum distance of $\mathcal{C}$

Subspace codes

R. Koetter, and F.R. Kschischang
Coding for errors and erasures in random network coding
IEEE Transaction on Information Theory, 2008.

$U, V \in \mathcal{G}_q(n, m)$: the set of m-dimensional $\mathbb{F}_q$ subspaces of $\mathbb{F}_{q^n}$

$$d(U, V) := \dim_{\mathbb{F}_q}(U) + \dim_{\mathbb{F}_q}(V) - 2\dim_{\mathbb{F}_q}(U \cap V)$$

$\mathcal{C} \subset \mathcal{G}_q(n, m)$, $(\mathcal{C}, d)$ *Constant dimension subspace code*

$$d(\mathcal{C}) := \min\{d(U, V) \ : \ U, V \in \mathcal{C}, U \neq V\}$$

minimum distance of $\mathcal{C}$

parameters of $\mathcal{C}$ $[n, d(\mathcal{C}), |\mathcal{C}|, m]_q$

Cyclic subspace codes

$\mathcal{C} \subseteq \mathcal{G}_q(n, m)$ is cyclic if

$$\forall \alpha \in \mathbb{F}_{q^n}^*, \forall V \in \mathcal{C} \quad \Longrightarrow \quad \alpha V \in \mathcal{C}$$

Cyclic subspace codes

$\mathcal{C} \subseteq \mathcal{G}_q(n, m)$ is cyclic if

$$\forall \alpha \in \mathbb{F}_{q^n}^*, \forall V \in \mathcal{C} \quad \Longrightarrow \quad \alpha V \in \mathcal{C}$$

$$\Updownarrow$$

$$\mathcal{C} = \cup_V Orb(V) = \cup_V \{\alpha V \ : \ \alpha \in \mathbb{F}_{q^n}^*\}$$

Cyclic subspace codes

$\mathcal{C} \subseteq \mathcal{G}_q(n, m)$ is cyclic if

$$\forall \alpha \in \mathbb{F}_{q^n}^*, \forall V \in \mathcal{C} \quad \Longrightarrow \quad \alpha V \in \mathcal{C}$$

$$\Updownarrow$$

$$\mathcal{C} = \cup_V Orb(V) = \cup_V \{\alpha V \ : \ \alpha \in \mathbb{F}_{q^n}^*\}$$

$\mathcal{C} = Orb(V)$ one orbit cyclic subspace code

Cyclic subspace codes

$\mathcal{C} \subseteq \mathcal{G}_q(n, m)$ is cyclic if

$$\forall \alpha \in \mathbb{F}_{q^n}^*, \ \forall V \in \mathcal{C} \quad \Longrightarrow \quad \alpha V \in \mathcal{C}$$

$$\Updownarrow$$

$$\mathcal{C} = \cup_V Orb(V) = \cup_V \{\alpha V \ : \ \alpha \in \mathbb{F}_{q^n}^*\}$$

$\mathcal{C} = Orb(V)$ one orbit cyclic subspace code

$\mathcal{C} = Orb(V)$ $[n, 2m - 2M, \frac{q^n - 1}{q^s - 1}, k]_q$

Cyclic subspace codes

$\mathcal{C} \subseteq \mathcal{G}_q(n, m)$ is cyclic if

$$\forall \alpha \in \mathbb{F}_{q^n}^*, \forall V \in \mathcal{C} \quad \Longrightarrow \quad \alpha V \in \mathcal{C}$$

$$\Updownarrow$$

$$\mathcal{C} = \cup_V Orb(V) = \cup_V \{\alpha V \ : \ \alpha \in \mathbb{F}_{q^n}^*\}$$

$\mathcal{C} = Orb(V)$ one orbit cyclic subspace code

$$\mathcal{C} = Orb(V) \quad [n, 2m - 2M, \tfrac{q^n-1}{q^s-1}, k]_q$$

$$M := \max\{\dim(\alpha V \cap \beta V) \ : \ \alpha, \beta \in \mathbb{F}_{q^n}^*, \alpha V \neq \beta V\}$$
$$s := \max\{t \mid n \ : \ V \quad \text{is} \quad \mathbb{F}_{q^t} - linear\}$$

One-Orbit Cyclic Subspace Codes

A.-L. Trautmann, F. Manganiello, M. Braun and J. Rosenthal
Cyclic orbit codes
IEEE Transaction on Information Theory, 2013.

One-Orbit Cyclic Subspace Codes

A.-L. Trautmann, F. Manganiello, M. Braun and J. Rosenthal
Cyclic orbit codes
IEEE Transaction on Information Theory, 2013.

Case 1: M=0 $\Rightarrow s = m$

$$\mathbb{F}_{q^m} \leq \mathbb{F}_{q^n}, \mathbb{F}_{q^m} \in \mathcal{G}_q(n, m), \mathcal{C} = Orb(\mathbb{F}_{q^m})$$

One-Orbit Cyclic Subspace Codes

A.-L. Trautmann, F. Manganiello, M. Braun and J. Rosenthal
Cyclic orbit codes
IEEE Transaction on Information Theory, 2013.

Case 1: M=0 $\Rightarrow s = m$

$$\mathbb{F}_{q^m} \leq \mathbb{F}_{q^n}, \mathbb{F}_{q^m} \in \mathcal{G}_q(n, m), \mathcal{C} = Orb(\mathbb{F}_{q^m})$$

$\mathcal{C}$ one-orbit cyclic subspace code $\longrightarrow [n, 2m, \frac{q^n-1}{q^m-1}, m]_q$

One-Orbit Cyclic Subspace Codes

A.-L. Trautmann, F. Manganiello, M. Braun and J. Rosenthal
Cyclic orbit codes
IEEE Transaction on Information Theory, 2013.

Case 1: M=0 $\Rightarrow s = m$

$$\mathbb{F}_{q^m} \leq \mathbb{F}_{q^n},\, \mathbb{F}_{q^m} \in \mathcal{G}_q(n, m),\, \mathcal{C} = Orb(\mathbb{F}_{q^m})$$

$\mathcal{C}$ one-orbit cyclic subspace code $\longrightarrow [n, 2m, \frac{q^n-1}{q^m-1}, m]_q$

spread code

One-Orbit Cyclic Subspace Codes

A.-L. Trautmann, F. Manganiello, M. Braun and J. Rosenthal
Cyclic orbit codes
IEEE Transaction on Information Theory, 2013.

Case 1: M=0 $\Rightarrow s = m$

$$\mathbb{F}_{q^m} \leq \mathbb{F}_{q^n},\ \mathbb{F}_{q^m} \in \mathcal{G}_q(n,m),\ \mathcal{C} = Orb(\mathbb{F}_{q^m})$$

$\mathcal{C}$ one-orbit cyclic subspace code $\longrightarrow [n, 2m, \frac{q^n-1}{q^m-1}, m]_q$
spread code

Next Case $\longrightarrow$ M=1 (and s=1)

Problem: To look for
$\mathcal{C}$ one-orbit cyclic subspace code $\longrightarrow [n, 2m-2, \frac{q^n-1}{q-1}, m]_q$

Optimal one-orbit cuclic subspace codes

Next Case $\longrightarrow$ M=1 (and s=1)

Problem: To look for

$\mathcal{C}$ one-orbit cyclic subspace code $\longrightarrow$ $[n, 2m-2, \frac{q^n-1}{q-1}, m]_q$

Conjecture (A.-L. Trautmann, F. Manganiello, M. Braun and J. Rosenthal)

For any prime power q and positive integers m, there exists a cyclic subspace code $\mathcal{C} \subset \mathcal{G}_q(n, m)$ of minimum distance $2m-2$ and size $\frac{q^n-1}{q-1}$.

Optimal one-orbit cyclic subspace codes

Next Case $\longrightarrow$ M=1 (and s=1)

Problem: To look for
$\mathcal{C}$ one-orbit cyclic subspace code $\longrightarrow$ $[n, 2m-2, \frac{q^n-1}{q-1}, m]_q$

E. Ben-Sasson, T. Etzion, A. Gabizon and N. Raviv
Subspace polynomials and cyclic subspace codes
IEEE Transaction on Information Theory, 2016.

Optimal one-orbit cyclic subspace codes

Next Case $\longrightarrow$ M=1 (and s=1)

Problem: To look for
$\mathcal{C}$ one-orbit cyclic subspace code $\longrightarrow$ $[n, 2m-2, \frac{q^n-1}{q-1}, m]_q$

E. Ben-Sasson, T. Etzion, A. Gabizon and N. Raviv
Subspace polynomials and cyclic subspace codes
IEEE Transaction on Information Theory, 2016.
K. Otal and F. Özbudak
Cyclic subspace codes via subspace polynomials
Des. Codes Cryptogr., 2017.

Optimal one-orbit cyclic subspace codes

Next Case $\longrightarrow$ M=1 (and s=1)

Problem: To look for

$\mathcal{C}$ one-orbit cyclic subspace code $\longrightarrow$ $[n, 2m-2, \frac{q^n-1}{q-1}, m]_q$

E. Ben-Sasson, T. Etzion, A. Gabizon and N. Raviv
Subspace polynomials and cyclic subspace codes
IEEE Transaction on Information Theory, 2016.
K. Otal and F. Özbudak
Cyclic subspace codes via subspace polynomials
Des. Codes Cryptogr., 2017.
R.M. Roth, N. Raviv and I. Tamo
Construction of Sidon spaces with applications to coding
IEEE Transaction on Information Theory, 2017.

Case M=1

Problem: To look for

$\mathcal{C}$ one-orbit cyclic subspace code $\longrightarrow$ $[n, 2m-2, \frac{q^n-1}{q-1}, m]_q$

M=1 $\Longleftrightarrow$ $\dim(\alpha V \cap \beta V) \leqslant 1$ for any $\alpha V \neq \beta V$

Case M=1

Problem: To look for

$\mathcal{C}$ one-orbit cyclic subspace code $\longrightarrow$ $[n, 2m-2, \frac{q^n-1}{q-1}, m]_q$

M=1 $\Longleftrightarrow \dim(\alpha V \cap \beta V) \leqslant 1$ for any $\alpha V \neq \beta V$

C. Bachoc, O. Serra, G. Zémor
An analogue of Vosper's theorem for extension fields
Mathematical Proceedings of the Cambridge Philosophical Society, 2017.

Property (C. Bachoc, O. Serra, G. Zémor)

$V \in \mathcal{G}_q(n, m)$

$$\dim(\alpha V \cap \beta V) \leqslant 1 \text{ for any } \alpha V \neq \beta V$$

$$\Updownarrow$$

for every $a, b, c, d \in V$,

$$ab = cd \quad \Longrightarrow \quad \{a\mathbb{F}_q, b\mathbb{F}_q\} = \{c\mathbb{F}_q, d\mathbb{F}_q\}$$

Case M=1

Problem: To look for

$\mathcal{C}$ one-orbit cyclic subspace code $\longrightarrow$ $[n, 2m-2, \frac{q^n-1}{q-1}, m]_q$

M=1 $\Longleftrightarrow$ $\dim(\alpha V \cap \beta V) \leqslant 1$ for any $\alpha V \neq \beta V$

C. Bachoc, O. Serra, G. Zémor
An analogue of Vosper's theorem for extension fields
Mathematical Proceedings of the Cambridge Philosophical Society, 2017.

Property (C. Bachoc, O. Serra, G. Zémor)

$V \in \mathcal{G}_q(n, m)$

$$\dim(\alpha V \cap \beta V) \leqslant 1 \text{ for any } \alpha V \neq \beta V$$

$$\Updownarrow$$

for every $a, b, c, d \in V$,

$ab = cd \quad \Longrightarrow \quad \{a\mathbb{F}_q, b\mathbb{F}_q\} = \{c\mathbb{F}_q, d\mathbb{F}_q\} \Rightarrow$ V is a *Sidon space*

Sidon spaces and optimal one-orbit subspace codes

Property (R.M. Roth, N. Raviv, I. Tamo 2017)

$$V \in \mathcal{G}_q(n, m)$$

$$V \text{ Sidon space} \iff \mathcal{C} = \mathrm{Orb}(V), \quad [n, 2m-2, \tfrac{q^n-1}{q-1}, m]_q.$$

Sidon spaces and optimal one-orbit subspace codes

Property (R.M. Roth, N. Raviv, I. Tamo 2017)

$$V \in \mathcal{G}_q(n, m)$$

$$V \text{ Sidon space} \iff \mathcal{C} = \mathrm{Orb}(V), \quad [n, 2m-2, \tfrac{q^n-1}{q-1}, m]_q.$$

This property allowed the authors to

1. Prove the Conjecture **(T.M.B.R.2013)** for most of the cases
2. Provide Explicit Constructions of One-Orbit Cyclic Subspace Codes via Explicit Constructions of Sidon Spaces

Our goals

1. Equivalence of Sidon Spaces via Equivalence of One-Orbit Subspace Codes

Our goals

1. Equivalence of Sidon Spaces via Equivalence of One-Orbit Subspace Codes
2. *New* Constructions of One-Orbit Cyclic Subspace Codes via *New* Constructions of Sidon Spaces

One-Orbit cyclic subspace codes from Sidon spaces

$S \in \mathcal{G}_q(n, m)$,

S Sidon space $\iff$ $\mathcal{C} = \mathrm{Orb}(S)$, $[n, 2m-2, \frac{q^n-1}{q-1}, m]_q$.

One-Orbit cyclic subspace codes from Sidon spaces

$S \in \mathcal{G}_q(n, m)$,

S Sidon space $\iff$ $\mathcal{C} = \mathrm{Orb}(S)$, $[n, 2m-2, \frac{q^n-1}{q-1}, m]_q$.

Properties

$\mathrm{Orb}(S)$, $S \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}$,

One-Orbit cyclic subspace codes from Sidon spaces

$S \in \mathcal{G}_q(n, m)$,

S Sidon space $\iff$ $\mathcal{C} = \mathrm{Orb}(S)$, $[n, 2m-2, \frac{q^n-1}{q-1}, m]_q$.

Properties

$\mathrm{Orb}(S)$, $S \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}$,

One-Orbit cyclic subspace codes from Sidon spaces

$$S \in \mathcal{G}_q(n, m),$$
$$S \text{ Sidon space} \iff \quad \mathcal{C} = \mathrm{Orb}(S), \quad [n, 2m-2, \tfrac{q^n-1}{q-1}, m]_q.$$

Properties

$\mathrm{Orb}(S), \quad S \leq_{\mathbb{F}_q} \mathbb{F}_{q^n},$

1. S Sidon space, $S' \leq_{\mathbb{F}_q} S \implies S'$ Sidon space

One-Orbit cyclic subspace codes from Sidon spaces

$S \in \mathcal{G}_q(n, m)$,

S Sidon space $\iff$ $\mathcal{C} = \mathrm{Orb}(S)$, $[n, 2m-2, \frac{q^n-1}{q-1}, m]_q$.

Properties

$\mathrm{Orb}(S)$, $S \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}$, $S^2 =< a \cdot b \, : \, a, b \in S >_{\mathbb{F}_q}$

1. S Sidon space, $S' \leq_{\mathbb{F}_q} S \implies S'$ Sidon space
2. S Sidon space

One-Orbit cyclic subspace codes from Sidon spaces

$S \in \mathcal{G}_q(n, m)$,

S Sidon space $\iff \quad \mathcal{C} = \mathrm{Orb}(S), \quad [n, 2m-2, \frac{q^n-1}{q-1}, m]_q$.

Properties

$\mathrm{Orb}(S), \quad S \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}, \quad S^2 =< a \cdot b \; : \; a, b \in S >_{\mathbb{F}_q}$

1. S Sidon space, $S' \leq_{\mathbb{F}_q} S \implies S'$ Sidon space
2. S Sidon space $\quad \implies \quad 2\dim S - 1 \leq \dim S^2 \leq \binom{\dim S+1}{2}$

One-Orbit cyclic subspace codes from Sidon spaces

$S \in \mathcal{G}_q(n, m)$,

S Sidon space $\iff \quad \mathcal{C} = \mathrm{Orb}(S), \quad [n, 2m-2, \frac{q^n-1}{q-1}, m]_q$.

Properties

$\mathrm{Orb}(S), \quad S \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}, \quad S^2 =< a \cdot b \, : \, a, b \in S >_{\mathbb{F}_q}$

1. S Sidon space, $S' \leq_{\mathbb{F}_q} S \implies S'$ Sidon space
2. S Sidon space $\implies 2\dim S - 1 \leq \dim S^2 \leq \binom{\dim S + 1}{2}$
3. S Sidon space, $\dim S \geq 3 \implies \dim S^2 \geq 2\dim S$ **B.S.Z. 2017**

One-Orbit cyclic subspace codes from Sidon spaces

$S \in \mathcal{G}_q(n, m)$,

S Sidon space $\iff$ $\mathcal{C} = \mathrm{Orb}(S)$, $[n, 2m-2, \frac{q^n-1}{q-1}, m]_q$.

Properties

$\mathrm{Orb}(S)$, $S \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}$, $S^2 =< a \cdot b \ : \ a, b \in S >_{\mathbb{F}_q}$

1. S Sidon space, $S' \leq_{\mathbb{F}_q} S \implies S'$ Sidon space
2. S Sidon space $\implies$ $2\dim S - 1 \leq \dim S^2 \leq \binom{\dim S+1}{2}$
3. S Sidon space, $\dim S \geq 3 \implies \dim S^2 \geq 2\dim S$ **B.S.Z. 2017**
4. S Sidon space and $\dim S \geq 3 \implies \dim S \leq \frac{n}{2}$

One-Orbit cyclic subspace codes from Sidon spaces

$S \in \mathcal{G}_q(n, m)$,

S Sidon space $\iff$ $\mathcal{C} = \mathrm{Orb}(S)$, $[n, 2m-2, \frac{q^n-1}{q-1}, m]_q$.

Properties

$\mathrm{Orb}(S)$, $S \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}$, $S^2 =< a \cdot b \ : \ a, b \in S >_{\mathbb{F}_q}$

1. S Sidon space, $S' \leq_{\mathbb{F}_q} S \implies S'$ Sidon space
2. S Sidon space $\implies$ $2\dim S - 1 \leq \dim S^2 \leq \binom{\dim S + 1}{2}$
3. S Sidon space, $\dim S \geq 3 \implies \dim S^2 \geq 2\dim S$ **B.S.Z. 2017**
4. S Sidon space and $\dim S \geq 3 \implies \dim S \leq \frac{n}{2}$
5. $\dim S^2 = \binom{\dim S + 1}{2} \implies S$ Sidon space

One-Orbit cyclic subspace codes from Sidon spaces

$S \in \mathcal{G}_q(n, m)$,

S Sidon space $\iff$ $\mathcal{C} = \mathrm{Orb}(S)$, $[n, 2m-2, \frac{q^n-1}{q-1}, m]_q$.

Properties

$\mathrm{Orb}(S)$, $S \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}$, $S^2 =< a \cdot b \; : \; a, b \in S >_{\mathbb{F}_q}$

1. S Sidon space, $S' \leq_{\mathbb{F}_q} S \implies S'$ Sidon space
2. S Sidon space $\implies 2\dim S - 1 \leq \dim S^2 \leq \binom{\dim S + 1}{2}$
3. S Sidon space, $\dim S \geq 3 \implies \dim S^2 \geq 2 \dim S$ **B.S.Z. 2017**
4. S Sidon space and $\dim S \geq 3 \implies \dim S \leq \frac{n}{2}$
5. $\dim S^2 = \binom{\dim S + 1}{2} \implies S$ Sidon space *Max span Sidon space*

Equivalence of One-orbit Cyclic Subspace Codes

H. Gluesing-Luerssen and H. Lehmann
Automorphism groups and isometries for cyclic orbit codes
Advances in Mathematics of Communications, 2023.

$U, V \in \mathcal{G}_q(n, m)$

$\mathrm{Orb}(U)$ and $\mathrm{Orb}(V)$ are semilinearly equivalent if

$$\mathrm{Orb}(U) = \mathrm{Orb}(V^\sigma)$$

where $\sigma \in \mathrm{Aut}(\mathbb{F}_{q^n})$.

Equivalence of One-orbit Cyclic Subspace Codes

H. Gluesing-Luerssen and H. Lehmann
Automorphism groups and isometries for cyclic orbit codes
Advances in Mathematics of Communications, 2023.

$U, V \in \mathcal{G}_q(n, m)$

$\mathrm{Orb}(U)$ and $\mathrm{Orb}(V)$ are semilinearly equivalent if

$$\mathrm{Orb}(U) = \mathrm{Orb}(V^\sigma)$$

where $\sigma \in \mathrm{Aut}(\mathbb{F}_{q^n})$.

Definition

U and V are semilinearly equivalent if there exists

$(\alpha, \sigma) \in \mathbb{F}_{q^n}^* \times \mathrm{Aut}(\mathbb{F}_{q^n})$ such that

$$U = \alpha V^\sigma.$$

Some invariants

$$\mathcal{C} = \mathrm{Orb}(S), \quad S \leqslant_q \mathbb{F}_{q^n} \quad \dim S = m$$

The following integers are invariant under semilinear equivalence:

Some invariants

$$\mathcal{C} = \mathrm{Orb}(S), \quad S \leqslant_q \mathbb{F}_{q^n} \quad \dim S = m$$

The following integers are invariant under semilinear equivalence:

1. $\dim S^2$

Some invariants

$$\mathcal{C} = \mathrm{Orb}(S), \quad S \leqslant_q \mathbb{F}_{q^n} \quad \dim S = m$$

The following integers are invariant under semilinear equivalence:

1. $\dim S^2$
2. $\delta_k(S) := \dim_{\mathbb{F}_{q^k}} < S >_{\mathbb{F}_{q^k}}$, where $k \mid n$

Some invariants

$$\mathcal{C} = \mathrm{Orb}(S), \quad S \leqslant_q \mathbb{F}_{q^n} \quad \dim S = m$$

The following integers are invariant under semilinear equivalence:

1. $\dim S^2$
2. $\delta_k(S) := \dim_{\mathbb{F}_{q^k}} < S >_{\mathbb{F}_{q^k}}$, where $k \mid n$
3. $w(F_S)$ is the weight of F_S, i.e. the number of non-zero coefficients of F_S the monic q-polynomial of q-degree m such that $\ker F_S = S$

Some invariants

$$\mathcal{C} = \mathrm{Orb}(S), \quad S \leqslant_q \mathbb{F}_{q^n} \quad \dim S = m$$

The following integers are invariant under semilinear equivalence:

1. $\dim S^2 \quad \longrightarrow \quad \dim S \geq 3$ and S Sidon space $\Rightarrow 2m \leq \dim S^2 \leq \binom{m+1}{2}$
2. $\delta_k(S) := \dim_{\mathbb{F}_{q^k}} < S >_{\mathbb{F}_{q^k}}$, where $k \mid n$
   S is generic $\Rightarrow 2 \leq \delta_k(S) \leq n/k$
3. $w(F_S)$ is the weight of F_S, i.e. the number of non-zero coefficients of F_S the monic q-polynomial of q-degree m such that $\ker F_S = S \longrightarrow w(F_S) \leq m + 1$

Sidon spaces with $\delta_k(S) = 2$

$V \in \mathcal{G}_q(n, m)$: $\delta_k(V) = 2$ where $k \mid n$ and V is *generic* in $\mathbb{F}_{q^n}$

Sidon spaces with $\delta_k(S) = 2$

$V \in \mathcal{G}_q(n, m)$: $\delta_k(V) = 2$ where $k \mid n$ and V is *generic* in $\mathbb{F}_{q^n}$

Standard form

$$V = V_{U,\gamma} = \{u + v\gamma \,:\, (u, v) \in U\} \subseteq \mathbb{F}_{q^k} + \gamma\mathbb{F}_{q^k}$$

Sidon spaces with $\delta_k(S) = 2$

$V \in \mathcal{G}_q(n, m)$: $\delta_k(V) = 2$ where $k \mid n$ and V is *generic* in $\mathbb{F}_{q^n}$

Standard form

$$V = V_{U,\gamma} = \{u + v\gamma \,:\, (u, v) \in U\} \subseteq \mathbb{F}_{q^k} + \gamma\mathbb{F}_{q^k}$$

$$\mathbb{F}_{q^k}(\gamma) = \mathbb{F}_{q^n}, \quad U \leq_{\mathbb{F}_q} \mathbb{F}_{q^k} \times \mathbb{F}_{q^k}, \quad \dim_{\mathbb{F}_q} U = m$$

Sidon spaces with $\delta_k(S) = 2$

$V \in \mathcal{G}_q(n, m)$: $\quad \delta_k(V) = 2$ where $k \mid n$ and V is *generic* in $\mathbb{F}_{q^n}$

Standard form

$$V = V_{U,\gamma} = \{u + v\gamma \, : \, (u, v) \in U\} \subseteq \mathbb{F}_{q^k} + \gamma \mathbb{F}_{q^k}$$

$$\mathbb{F}_{q^k}(\gamma) = \mathbb{F}_{q^n}, \quad U \leq_{\mathbb{F}_q} \mathbb{F}_{q^k} \times \mathbb{F}_{q^k}, \quad \dim_{\mathbb{F}_q} U = m$$

$$V = V_{U,\gamma} \text{ Sidon space} \quad \Longrightarrow \quad m = \dim_{\mathbb{F}_q} V = \dim_{\mathbb{F}_q} U \leq k$$

k-dimensional Sidon spaces with $\delta_k(S) = 2$

Theorem

$V \in \mathcal{G}_q(n, k), \quad \delta_k(V) = 2$

$$V = V_{f,\gamma} = \{u + f(u)\gamma \,:\, u \in \mathbb{F}_{q^k}\} \subseteq \mathbb{F}_{q^k}(\gamma)$$

k-dimensional Sidon spaces with $\delta_k(S) = 2$

Theorem

$V \in \mathcal{G}_q(n, k)$, $\quad \delta_k(V) = 2$

$$V = V_{f,\gamma} = \{u + f(u)\gamma \,:\, u \in \mathbb{F}_{q^k}\} \subseteq \mathbb{F}_{q^k}(\gamma)$$

$$f(x) = \sum_{i=0}^{k-1} a_i x^{q^i} \in \mathcal{L}_{k,q}$$

k-dimensional Sidon spaces with $\delta_k(S) = 2$

Theorem

$$[\mathbb{F}_{q^k}(\gamma) : \mathbb{F}_{q^k}] > 2$$

$$V_{f,\gamma} \text{ is a Sidon space in } \mathbb{F}_{q^k}(\gamma)$$

$$\Updownarrow$$

$$S_{u,f} \cap S_{v,f} = \mathbb{F}_q$$

$$\forall u, v \in \mathbb{F}^*_{q^k} \text{ such that } u\mathbb{F}_q \neq v\mathbb{F}_q$$
$$S_{u,f} = \{\lambda \in \mathbb{F}_{q^k} : f(\lambda u) - \lambda f(u) = 0\}.$$

Sidon polynomials in $\mathbb{F}_{q^k}$

Definition

f q-polynomial in $\mathbb{F}_{q^k}$
f is a Sidon polynomial if

$$S_{u,f} \cap S_{v,f} = \mathbb{F}_q,$$

$\forall u, v \in \mathbb{F}_{q^k}^*$ s.t. $u\mathbb{F}_q \neq v\mathbb{F}_q$
$S_{u,f} = \{\lambda \in \mathbb{F}_{q^k} \colon f(\lambda u) - \lambda f(u) = 0\}$.

Sidon polynomials in $\mathbb{F}_{q^k}$

Definition

f q-polynomial in $\mathbb{F}_{q^k}$
f is a Sidon polynomial if

$$S_{u,f} \cap S_{v,f} = \mathbb{F}_q,$$

$\forall u, v \in \mathbb{F}^*_{q^k}$ s.t. $u\mathbb{F}_q \neq v\mathbb{F}_q$
$S_{u,f} = \{\lambda \in \mathbb{F}_{q^k} : f(\lambda u) - \lambda f(u) = 0\}$.

Corollary

$$V_{f,\gamma} = \{u + f(u)\gamma \ : \ u \in \mathbb{F}_{q^k}\} \subset \mathbb{F}_{q^k}(\gamma)$$

$$[\mathbb{F}_{q^k}(\gamma) : \mathbb{F}_{q^k}] > 2$$

$V_{f,\gamma}$ is a Sidon space in $\mathbb{F}_{q^n}$ iff f is a Sidon polynomial in $\mathbb{F}_{q^k}$.

Sidon spaces with $\delta_k(S) = 2$ and semilinear equivalence

$$U_f = \{(u, f(u)) : u \in \mathbb{F}_{q^k}\} \qquad U_g = \{(u, g(u)) : u \in \mathbb{F}_{q^k}\}$$

Semilinear Equivalence in standard form

$$V_{f,\gamma} = \{u + f(u)\gamma : u \in \mathbb{F}_{q^k}\}$$
$$V_{g,\xi} = \{w + g(w)\xi : w \in \mathbb{F}_{q^k}\}$$

Sidon spaces with $\delta_k(S) = 2$ and semilinear equivalence

$$U_f = \{(u, f(u)) : u \in \mathbb{F}_{q^k}\} \qquad U_g = \{(u, g(u)) : u \in \mathbb{F}_{q^k}\}$$

Semilinear Equivalence in standard form

$$V_{f,\gamma} = \{u + f(u)\gamma : u \in \mathbb{F}_{q^k}\}$$
$$V_{g,\xi} = \{w + g(w)\xi : w \in \mathbb{F}_{q^k}\}$$

$V_{f,\gamma}$, $V_{g,\xi}$ semilinearly equivalent if and only if

$\exists A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, \mathbb{F}_{q^k})$ and $\sigma \in \mathrm{Aut}(\mathbb{F}_{q^n})$ such that

$$U_f^\sigma = \{wA : w \in U_g\} = U_g \cdot A$$
$$\xi = \frac{c + d\gamma^\sigma}{a + b\gamma^\sigma}$$

Sidon spaces with $\delta_k(S) = 2$ and semilinear equivalence

$$U_f = \{(u, f(u)) : u \in \mathbb{F}_{q^k}\} \qquad U_g = \{(u, g(u)) : u \in \mathbb{F}_{q^k}\}$$

Semilinear Equivalence in standard form

$$V_{f,\gamma} = \{u + f(u)\gamma : u \in \mathbb{F}_{q^k}\}$$
$$V_{g,\xi} = \{w + g(w)\xi : w \in \mathbb{F}_{q^k}\}$$

$V_{f,\gamma}$, $V_{g,\xi}$ semilinearly equivalent if and only if

$$\exists A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}(2, \mathbb{F}_{q^k}) \text{ and } \sigma \in \mathrm{Aut}(\mathbb{F}_{q^n}) \text{ such that}$$
$$U_f^\sigma = \{wA \colon w \in U_g\} = U_g \cdot A$$
$$\xi = \frac{c + d\gamma^\sigma}{a + b\gamma^\sigma}$$

U_f and U_g are $\Gamma L(2, q^k)$-equivalent

Sidon polynomials

Definition

$f \in \mathcal{L}_{k,q}$ is scattered if for any $a, b \in \mathbb{F}^*_{q^k}$ such that

$$f(a)/a = f(b)/b$$

Sidon polynomials

Definition

$f \in \mathcal{L}_{k,q}$ is scattered if for any $a, b \in \mathbb{F}_{q^k}^*$ such that

$$f(a)/a = f(b)/b \quad \Rightarrow \quad a/b \in \mathbb{F}_q$$

Sidon polynomials

Definition

$f \in \mathcal{L}_{k,q}$ is scattered if for any $a, b \in \mathbb{F}^*_{q^k}$ such that

$$f(a)/a = f(b)/b \quad \Rightarrow \quad a/b \in \mathbb{F}_q$$

Property

$f \in \mathcal{L}_{k,q}$ scattered polynomial $\Longrightarrow$ f Sidon polynomial.

Sidon polynomials

Definition

$f \in \mathcal{L}_{k,q}$ is scattered if for any $a, b \in \mathbb{F}^*_{q^k}$ such that

$$f(a)/a = f(b)/b \quad \Rightarrow \quad a/b \in \mathbb{F}_q$$

Property

$f \in \mathcal{L}_{k,q}$ scattered polynomial $\Longrightarrow$ f Sidon polynomial.

$$\not\Leftarrow$$

Known scattered polynomials

	k	$f(x)$	Conditions		$V_{f,\gamma}$
1)		x^{q^s}	$\gcd(s,k)=1$	2000	R.R.T.2017, L.L.2021 Z.T.2023, Z.T.2023
2)		$x^{q^s}+\delta x^{q^{s(k-1)}}$	$\gcd(s,k)=1$, $\mathrm{N}_{q^k/q}(\delta)\neq 1$	2001/2015	
3)	2ℓ	$x^{q^s}+x^{q^{s(\ell-1)}}+$ $\delta^{q^\ell+1}x^{q^{s(\ell+1)}}+\delta^{1-q^{2\ell-1}}x^{q^{s(2\ell-1)}}$	q odd, $\mathrm{N}_{q^{2\ell}/q^\ell}(\delta)=-1$, $\gcd(s,\ell)=1$	2020/2021/2022	
4)	6	$x^q+\delta x^{q^4}$	$q>4$, certain choices of δ	2018-2020	
5)	6	$x^q+x^{q^3}+\delta x^{q^5}$	q odd, $\delta^2+\delta=1$	2018-2020	
6)	8	$x^q+\delta x^{q^5}$	q odd, $\delta^2=-1$	2018	

Sidon spaces from binomials

Theorem

$$f(x) = x^{q^s} + \delta x^{q^l} \in \mathcal{L}_{k,q}, \text{ with } 1 \leq s < l$$

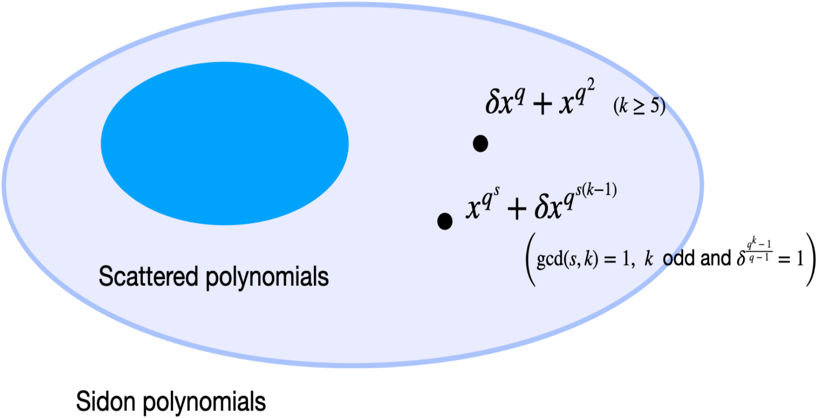
Sidon spaces from binomials

Theorem

$$f(x) = x^{q^s} + \delta x^{q^l} \in \mathcal{L}_{k,q}, \text{ with } 1 \leq s < l$$

1. $\gcd(k, l-s) = 1 \implies f$ is a Sidon polynomial.
2. $\gcd(k, l-s) = t > 1 \implies f$ is a Sidon polynomial iff f is a scattered polynomial

Sidon spaces from binomials



Comparison with known constructions of Sidon Spaces

$S \in \mathcal{G}_q(n, m),\ m \le k \mid n$ and $\delta_k(S) = 2$;

1. $S \in \mathcal{G}_q(n, m),\ m \le k \mid n$ such that $\delta_k(S) \ge 3$;
2. $S \in \mathcal{G}_q(n, m),\ m \le k \mid n$ as kernel of subspace polynomials with low weight;
3. $S \in \mathcal{G}_q(n, m)$, n possibly prime (mostly existence results)

Thank you for your attention!