Algebraic and geometric methods in the theory of subspace codes

Olga Polverino

Università degli Studi della Campania “Luigi Vanvitelli”

WCC 2026
The Fourteenth International Workshop on Coding and Cryptography
June 8-12, 2026, Paris (France)

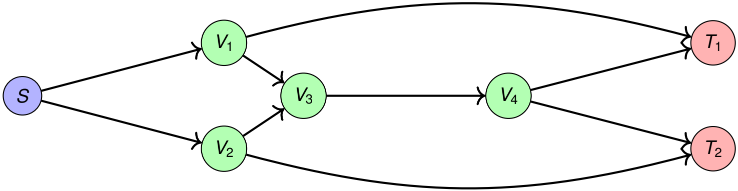
Outline

Network coding

R. Ahlswede, N. Cai, S. R. Li,: *Network Information Flow*, IEEE TRANSACTIONS ON INFORMATION THEORY, **2000**.

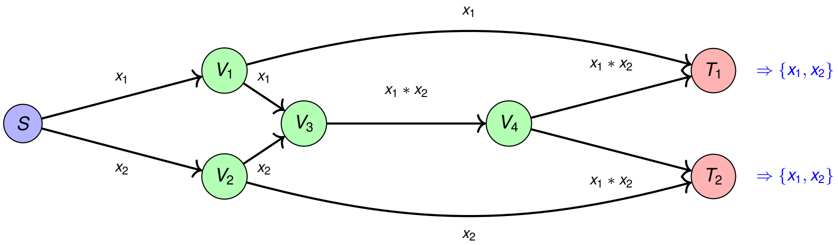
Network coding

R. Ahlswede, N. Cai, S. R. Li,: *Network Information Flow*, IEEE TRANSACTIONS ON INFORMATION THEORY, **2000**.



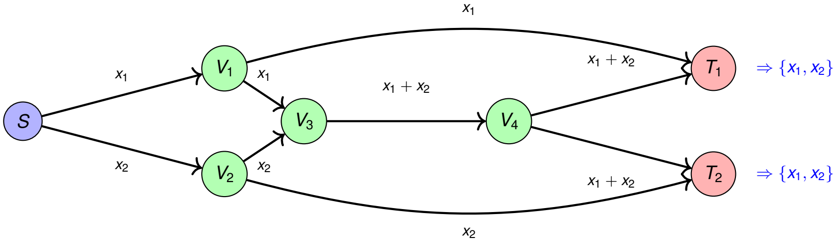
Network coding

R. Ahlswede, N. Cai, S. R. Li,: *Network Information Flow*, IEEE Transactions on Information Theory, **2000**.



Linear Network coding

S. R. Li, R.W. Yeung, N. Cai: *Linear Network Coding*, IEEE Transactions on Information Theory, **2003**.

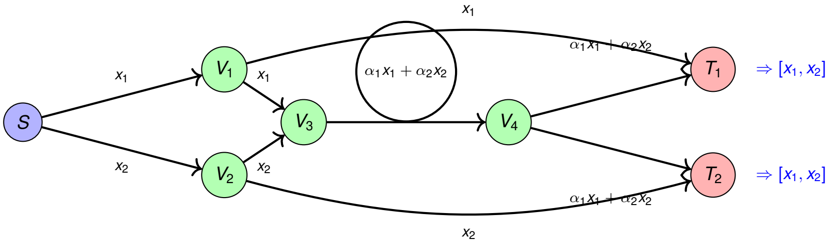


RLNC: Random Linear Network Coding

T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi and, B. Leong: *A random linear network coding approach to multicast* , IEEE Transactions on Information Theory, **2006**.

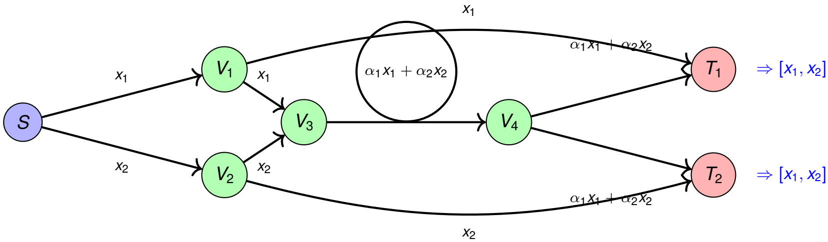
RLNC: Random Linear Network Coding

T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi and, B. Leong: *A random linear network coding approach to multicast* , IEEE Transactions on Information Theory, **2006**.



RLNC: Random Linear Network Coding

T. Ho, M. Médard, R. Koetter, D. R. Karger, M. Effros, J. Shi and, B. Leong: *A random linear network coding approach to multicast* , IEEE TRANSACTIONS ON INFORMATION THEORY, **2006**.



R. Koetter, and F.R. Kschischang : *Coding for errors and erasures in random network coding* , IEEE TRANSACTIONS ON INFORMATION THEORY, **2008**.

Subspace codes

$\mathbb{V}(n, q)$: vector space of dimension n over the finite field $\mathbb{F}_q$

Subspace codes

$\mathbb{V}(n,q)$: vector space of dimension n over the finite field $\mathbb{F}_q$

$\mathcal{P}_q(n)$: the set of $\mathbb{F}_q$-subspaces of $\mathbb{V}(n,q)$

Subspace codes

$\mathbb{V}(n, q)$: vector space of dimension n over the finite field $\mathbb{F}_q$

$\mathcal{P}_q(n)$: the set of $\mathbb{F}_q$-subspaces of $\mathbb{V}(n, q)$

Subspace codes

$\mathbb{V}(n,q)$: vector space of dimension n over the finite field $\mathbb{F}_q$

$\mathcal{P}_q(n)$: the set of $\mathbb{F}_q$-subspaces of $\mathbb{V}(n,q)$

$$(\mathcal{P}_q(n), d)$$

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

Subspace codes

$\mathbb{V}(n,q)$: vector space of dimension n over the finite field $\mathbb{F}_q$

$\mathcal{P}_q(n)$: the set of $\mathbb{F}_q$-subspaces of $\mathbb{V}(n,q)$

$(\mathcal{P}_q(n), d)$

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

$\mathcal{C} \subseteq \mathcal{P}_q(n)$, $(\mathcal{C}, d)$ *Subspace code*

Subspace codes

$\mathbb{V}(n,q)$: vector space of dimension n over the finite field $\mathbb{F}_q$

$\mathcal{P}_q(n)$: the set of $\mathbb{F}_q$-subspaces of $\mathbb{V}(n,q)$

$\mathcal{G}_q(n,k) \subseteq \mathcal{P}_q(n)$: the set of k-dimensional $\mathbb{F}_q$-subspaces of $\mathbb{V}(n,q)$

$$(\mathcal{P}_q(n), d)$$

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

$\mathcal{C} \subseteq \mathcal{P}_q(n)$, $(\mathcal{C}, d)$ *Subspace code*

$$(\mathcal{G}_q(n,k), d)$$

$$d(U,W) = 2k - 2\dim_{\mathbb{F}_q}(U \cap W)$$

Subspace codes

$\mathbb{V}(n,q)$: vector space of dimension n over the finite field $\mathbb{F}_q$

$\mathcal{P}_q(n)$: the set of $\mathbb{F}_q$-subspaces of $\mathbb{V}(n,q)$

$\mathcal{G}_q(n,k) \subseteq \mathcal{P}_q(n)$: the set of k-dimensional $\mathbb{F}_q$-subspaces of $\mathbb{V}(n,q)$

$(\mathcal{P}_q(n), d)$

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

$\mathcal{C} \subseteq \mathcal{P}_q(n)$, $(\mathcal{C}, d)$ *Subspace code*

$(\mathcal{G}_q(n,k), d)$

$d(U,W) = 2k - 2\dim_{\mathbb{F}_q}(U \cap W)$

$\mathcal{C} \subseteq \mathcal{G}_q(n,k)$, $(\mathcal{C}, d)$ *Constant dimension Subspace code*

Subspace codes

$\mathbb{V}(n,q)$: vector space of dimension n over the finite field $\mathbb{F}_q$

$\mathcal{P}_q(n)$: the set of $\mathbb{F}_q$-subspaces of $\mathbb{V}(n,q)$

$\mathcal{G}_q(n,k) \subseteq \mathcal{P}_q(n)$: the set of k-dimensional $\mathbb{F}_q$-subspaces of $\mathbb{V}(n,q)$

$(\mathcal{P}_q(n), d)$

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

$\mathcal{C} \subseteq \mathcal{P}_q(n)$, $(\mathcal{C}, d)$ *Subspace code*

$(\mathcal{G}_q(n,k), d)$

$$d(U,W) = 2k - 2\dim_{\mathbb{F}_q}(U \cap W)$$

$\mathcal{C} \subseteq \mathcal{G}_q(n,k)$, $(\mathcal{C}, d)$ *Constant dimension Subspace code*

parameters of $\mathcal{C}$ $\quad (n, d(\mathcal{C}), |\mathcal{C}|)_q$

Subspace codes

$\mathbb{V}(n,q)$: vector space of dimension n over the finite field $\mathbb{F}_q$

$\mathcal{P}_q(n)$: the set of $\mathbb{F}_q$-subspaces of $\mathbb{V}(n,q)$

$\mathcal{G}_q(n,k) \subseteq \mathcal{P}_q(n)$: the set of k-dimensional $\mathbb{F}_q$-subspaces of $\mathbb{V}(n,q)$

$(\mathcal{P}_q(n), d)$

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

$\mathcal{C} \subseteq \mathcal{P}_q(n)$, $(\mathcal{C}, d)$ *Subspace code*

parameters of $\mathcal{C}$ $\quad (n, d(\mathcal{C}), |\mathcal{C}|)_q$

$(\mathcal{G}_q(n,k), d)$

$d(U,W) = 2k - 2\dim_{\mathbb{F}_q}(U \cap W)$

$\mathcal{C} \subseteq \mathcal{G}_q(n,k)$, $(\mathcal{C}, d)$ *Constant dimension Subspace code*

parameters of $\mathcal{C}$ $\quad (n, d(\mathcal{C}), |\mathcal{C}|, k)_q$

Subspace codes

$\mathbb{V}(n,q)$: vector space of dimension n over the finite field $\mathbb{F}_q$

$\mathcal{P}_q(n)$: the set of $\mathbb{F}_q$-subspaces of $\mathbb{V}(n,q)$

$\mathcal{G}_q(n,k) \subseteq \mathcal{P}_q(n)$: the set of k-dimensional $\mathbb{F}_q$-subspaces of $\mathbb{V}(n,q)$

$$(\mathcal{P}_q(n), d)$$

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

$\mathcal{C} \subseteq \mathcal{P}_q(n)$, $(\mathcal{C}, d)$ *Subspace code*

parameters of $\mathcal{C}$ $\quad (n, d(\mathcal{C}), |\mathcal{C}|)_q$

$$(\mathcal{G}_q(n,k), d)$$

$$d(U,W) = 2k - 2\dim_{\mathbb{F}_q}(U \cap W)$$

$\mathcal{C} \subseteq \mathcal{G}_q(n,k)$, $(\mathcal{C}, d)$ *Constant dimension Subspace code*

parameters of $\mathcal{C}$ $\quad (n, d(\mathcal{C}), |\mathcal{C}|, k)_q$

$A_q(n,d;k)$ size of the largest subspace code in $\mathcal{G}_q(n,k)$ with minimum distance d

Subspace codes

$\mathbb{V}(n,q)$: vector space of dimension n over the finite field $\mathbb{F}_q$

$\mathcal{P}_q(n)$: the set of $\mathbb{F}_q$-subspaces of $\mathbb{V}(n,q)$

$\mathcal{G}_q(n,k) \subseteq \mathcal{P}_q(n)$: the set of k-dimensional $\mathbb{F}_q$-subspaces of $\mathbb{V}(n,q)$

$(\mathcal{P}_q(n), d)$

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

$\mathcal{C} \subseteq \mathcal{P}_q(n)$, $(\mathcal{C}, d)$ *Subspace code*

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

$(\mathcal{G}_q(n,k), d)$

$d(U,W) = 2k - 2\dim_{\mathbb{F}_q}(U \cap W)$

$\mathcal{C} \subseteq \mathcal{G}_q(n,k)$, $(\mathcal{C}, d)$ *Constant dimension Subspace code*

parameters of $\mathcal{C}$ $(n, d(\mathcal{C}), |\mathcal{C}|, k)_q$

$A_q(n,d;k)$ size of the largest subspace code in $\mathcal{G}_q(n,k)$ with minimum distance d $(d \in \{2,4,\dots,2k\})$

Linear isometries

$$\mathcal{C}, \mathcal{C}' \subseteq \mathcal{P}_q(n)$$

$\mathcal{C}$ and $\mathcal{C}'$ are linearly isometric if there exists

$\varphi \in GL(n, q)$ such that $\varphi(\mathcal{C}) = \mathcal{C}'$.

Linear isometries

$$\mathcal{C}, \mathcal{C}' \subseteq \mathcal{P}_q(n)$$

$\mathcal{C}$ and $\mathcal{C}'$ are linearly isometric if there exists

$\varphi \in GL(n, q)$ such that $\varphi(\mathcal{C}) = \mathcal{C}'$.

$$|\mathcal{C}| = |\mathcal{C}'| \quad d(\mathcal{C}) = d(\mathcal{C}')$$

Linear isometries

$$\mathcal{C}, \mathcal{C}' \subseteq \mathcal{P}_q(n)$$

$\mathcal{C}$ and $\mathcal{C}'$ are linearly isometric if there exists

$\varphi \in GL(n, q)$ such that $\varphi(\mathcal{C}) = \mathcal{C}'$.

$$|\mathcal{C}| = |\mathcal{C}'| \quad d(\mathcal{C}) = d(\mathcal{C}')$$

$$Aut(\mathcal{C}) = \{\varphi \in GL(n, q) \, : \, \varphi(\mathcal{C}) = \mathcal{C}\}$$

Dual subspace code

$$\mathcal{G}_q(n,k) \subseteq \mathcal{P}_q(n)$$

Dual subspace code

$$\mathcal{G}_q(n,k) \subseteq \mathcal{P}_q(n) \qquad \mathcal{G}_q(n,n-k) \subseteq \mathcal{P}_q(n)$$

Dual subspace code

$$\mathcal{G}_q(n,k) \subseteq \mathcal{P}_q(n) \qquad \mathcal{G}_q(n,n-k) \subseteq \mathcal{P}_q(n)$$

$$U \in \mathcal{G}_q(n,k) \xrightarrow{\perp} U^{\perp} \in \mathcal{G}_q(n,n-k)$$

Dual subspace code

$$\mathcal{G}_q(n,k) \subseteq \mathcal{P}_q(n) \qquad\qquad \mathcal{G}_q(n,n-k) \subseteq \mathcal{P}_q(n)$$

$$U \in \mathcal{G}_q(n,k) \xrightarrow{\quad\perp\quad} U^\perp \in \mathcal{G}_q(n,n-k)$$

$$d(U,W) = d(U^\perp, W^\perp)$$

Dual subspace code

$$\mathcal{G}_q(n,k) \subseteq \mathcal{P}_q(n) \qquad \mathcal{G}_q(n,n-k) \subseteq \mathcal{P}_q(n)$$

$$U \in \mathcal{G}_q(n,k) \xrightarrow{\perp} U^{\perp} \in \mathcal{G}_q(n,n-k)$$

$$d(U,W) = d(U^{\perp}, W^{\perp})$$

Dual subspace code

$$\mathcal{G}_q(n,k) \subseteq \mathcal{P}_q(n) \qquad \mathcal{G}_q(n,n-k) \subseteq \mathcal{P}_q(n)$$

$$U \in \mathcal{G}_q(n,k) \xrightarrow{\perp} U^\perp \in \mathcal{G}_q(n,n-k)$$

$$d(U,W) = d(U^\perp, W^\perp)$$

$\mathcal{C} \subseteq \mathcal{G}_q(n,k)$

$(n, d(\mathcal{C}), |\mathcal{C}|, k)_q$

Dual subspace code

$$\mathcal{G}_q(n,k) \subseteq \mathcal{P}_q(n) \qquad \mathcal{G}_q(n,n-k) \subseteq \mathcal{P}_q(n)$$

$$U \in \mathcal{G}_q(n,k) \xrightarrow{\ \perp\ } U^\perp \in \mathcal{G}_q(n,n-k)$$

$$d(U,W) = d(U^\perp, W^\perp)$$

$\mathcal{C} \subseteq \mathcal{G}_q(n,k)$
$(n, d(\mathcal{C}), |\mathcal{C}|, k)_q$

$\mathcal{C}^\perp \subseteq \mathcal{G}_q(n,n-k)$ dual of $\mathcal{C}$
$(n, d(\mathcal{C}^\perp), |\mathcal{C}^\perp|, n-k)_q$

Dual subspace code

$\mathcal{G}_q(n,k) \subseteq \mathcal{P}_q(n)$ $\mathcal{G}_q(n,n-k) \subseteq \mathcal{P}_q(n)$

$$U \in \mathcal{G}_q(n,k) \xrightarrow{\perp} U^\perp \in \mathcal{G}_q(n,n-k)$$

$$d(U,W) = d(U^\perp, W^\perp)$$

$\mathcal{C} \subseteq \mathcal{G}_q(n,k)$
$(n, d(\mathcal{C}), |\mathcal{C}|, k)_q$

$\mathcal{C}^\perp \subseteq \mathcal{G}_q(n,n-k)$ dual of $\mathcal{C}$
$(n, d(\mathcal{C}^\perp), |\mathcal{C}^\perp|, n-k)_q$

$$|\mathcal{C}| = |\mathcal{C}^\perp|, \quad d(\mathcal{C}) = d(\mathcal{C}^\perp)$$

Dual subspace code

$$\mathcal{G}_q(n,k) \subseteq \mathcal{P}_q(n) \qquad\qquad \mathcal{G}_q(n,n-k) \subseteq \mathcal{P}_q(n)$$

$$U \in \mathcal{G}_q(n,k) \xrightarrow{\perp} U^\perp \in \mathcal{G}_q(n,n-k)$$

$$d(U,W) = d(U^\perp, W^\perp)$$

$$\mathcal{C} \subseteq \mathcal{G}_q(n,k) \qquad\qquad \mathcal{C}^\perp \subseteq \mathcal{G}_q(n,n-k) \text{ dual of } \mathcal{C}$$

$$(n, d(\mathcal{C}), |\mathcal{C}|, k)_q \qquad\qquad (n, d(\mathcal{C}^\perp), |\mathcal{C}^\perp|, n-k)_q$$

$$|\mathcal{C}| = |\mathcal{C}^\perp|, \quad d(\mathcal{C}) = d(\mathcal{C}^\perp)$$

$$A_q(n,d;k) = A_q(n,d;n-k)$$

Dual subspace code

$$\mathcal{G}_q(n,k) \subseteq \mathcal{P}_q(n) \qquad\qquad \mathcal{G}_q(n,n-k) \subseteq \mathcal{P}_q(n)$$

$$U \in \mathcal{G}_q(n,k) \xrightarrow{\perp} U^{\perp} \in \mathcal{G}_q(n,n-k)$$

$$d(U,W) = d(U^{\perp},W^{\perp})$$

$\mathcal{C} \subseteq \mathcal{G}_q(n,k)$
$(n, d(\mathcal{C}), |\mathcal{C}|, k)_q$

$\mathcal{C}^{\perp} \subseteq \mathcal{G}_q(n,n-k)$ dual of $\mathcal{C}$
$(n, d(\mathcal{C}^{\perp}), |\mathcal{C}^{\perp}|, n-k)_q$

$$|\mathcal{C}| = |\mathcal{C}^{\perp}|, \qquad d(\mathcal{C}) = d(\mathcal{C}^{\perp})$$

$$A_q(n,d;k) = A_q(n,d;n-k) \longrightarrow k \leq \frac{n}{2}$$

Some bounds for $A_q(n, d, k)$

$$A_q(n, d; k),\ \delta := \frac{d}{2},\ e := \left\lfloor \frac{\delta - 1}{2} \right\rfloor \text{ and } k \leq \frac{n}{2}$$

Some bounds for $A_q(n, d, k)$

$$A_q(n, d; k),\ \delta := \frac{d}{2},\ e := \left\lfloor \frac{\delta - 1}{2} \right\rfloor \text{ and } k \leq \frac{n}{2}$$

Sphere Packing Bound **[Koetter-Kschischang** IEEE TIT**, 2008]**

$$A_q(n, d; k) \leq \frac{|\mathcal{G}_q(n, k)|}{|\mathcal{S}_{n,k}(U; e)|}$$

Some bounds for $A_q(n,d,k)$

$$A_q(n,d;k),\ \delta := \frac{d}{2},\ e := \left\lfloor \frac{\delta-1}{2} \right\rfloor \text{ and } k \leq \frac{n}{2}$$

Sphere Packing Bound [Koetter-Kschischang IEEE TIT, 2008]

$$A_q(n,d;k) \leq \frac{|\mathcal{G}_q(n,k)|}{|\mathcal{S}_{n,k}(U;e)|}$$

$$\mathcal{S}_{n,k}(U;e) = \{W \in \mathcal{G}_q(n,k) \ :\ d(U,W) \leq 2e\}$$

sphere of radius e centered in U

Some bounds for $A_q(n,d,k)$

$$A_q(n,d;k),\ \delta := \frac{d}{2},\ e := \left\lfloor \frac{\delta-1}{2} \right\rfloor \text{ and } k \leq \frac{n}{2}$$

Sphere Packing Bound **[Koetter-Kschischang** IEEE TIT**, 2008]**

$$A_q(n,d;k) \leq \frac{|\mathcal{G}_q(n,k)|}{|\mathcal{S}_{n,k}(U;e)|} = \frac{\begin{bmatrix} n \\ k \end{bmatrix}_q}{\sum_{i=0}^{e} q^{i^2} \begin{bmatrix} k \\ i \end{bmatrix}_q \begin{bmatrix} n-k \\ i \end{bmatrix}_q}$$

$$\mathcal{S}_{n,k}(U;e) = \{W \in \mathcal{G}_q(n,k) \ :\ d(U,W) \leq 2e\}$$

sphere of radius e centered in U

Anticode Bound

$$A_q(n, d; k),\ d = 2\delta \text{ and } k \leq \frac{n}{2}$$

Anticode Bound or Packing bound **[Etzion-Vardy** IEEE TIT**, 2011–Frankl-Wilson** JCTA**, 1986]**

$$A_q(n, d; k) \leq \frac{|\mathcal{G}_q(n,k)|}{|\mathcal{A}_{n,k}(Y;\delta-1)|}$$

Anticode Bound

$$A_q(n,d;k),\ d=2\delta \text{ and } k \leq \frac{n}{2}$$

Anticode Bound or Packing bound **[Etzion-Vardy** IEEE TIT**, 2011–Frankl-Wilson** JCTA**, 1986]**

$$A_q(n,d;k) \leq \frac{|\mathcal{G}_q(n,k)|}{|\mathcal{A}_{n,k}(Y;\delta-1)|}$$

$\mathcal{A}_{n,k}(Y;\delta-1)=\{W \in \mathcal{G}_q(n,k)\ :\ Y \subseteq W\}$ for $Y \in \mathcal{G}_q(n,k-\delta+1)$
anticode of diameter $\delta-1$ in $\mathcal{G}_q(n,k)$ of largest possible size

Anticode Bound

$$A_q(n, d; k),\ d = 2\delta \text{ and } k \leq \frac{n}{2}$$

Anticode Bound or Packing bound **[Etzion-Vardy** IEEE TIT, **2011–Frankl-Wilson** JCTA, **1986]**

$$A_q(n, d; k) \leq \frac{|\mathcal{G}_q(n,k)|}{|\mathcal{A}_{n,k}(Y;\delta-1)|} = \frac{\begin{bmatrix} n \\ k \end{bmatrix}_q}{\begin{bmatrix} n-k+\delta-1 \\ \delta-1 \end{bmatrix}_q}$$

$\mathcal{A}_{n,k}(Y; \delta - 1) = \{W \in \mathcal{G}_q(n, k) \ :\ Y \subseteq W\}$ for $Y \in \mathcal{G}_q(n, k - \delta + 1)$
anticode of diameter $\delta - 1$ in $\mathcal{G}_q(n, k)$ of largest possible size

Anticode Bound

$$A_q(n,d;k),\ d=2\delta \text{ and } k\leq \frac{n}{2}$$

Anticode Bound or Packing bound **[Etzion-Vardy** IEEE TIT, **2011–Frankl-Wilson** JCTA, **1986]**

$$A_q(n,d;k)\leq \frac{|\mathcal{G}_q(n,k)|}{|\mathcal{A}_{n,k}(Y;\delta-1)|}=\frac{\begin{bmatrix} n \\ k \end{bmatrix}_q}{\begin{bmatrix} n-k+\delta-1 \\ \delta-1 \end{bmatrix}_q}$$

$\mathcal{A}_{n,k}(Y;\delta-1)=\{W\in\mathcal{G}_q(n,k)\ :\ Y\subseteq W\}$ for $Y\in\mathcal{G}_q(n,k-\delta+1)$
anticode of diameter $\delta-1$ in $\mathcal{G}_q(n,k)$ of largest possible size

$$\mathcal{P}=\{(Y,W)\ :\ Y\in\mathcal{G}_q(n,k-\delta+1),\ W\in\mathcal{C}\ :\ Y\subseteq W\}$$

Anticode Bound

$$A_q(n,d;k),\ d = 2\delta \text{ and } k \leq \frac{n}{2}$$

Anticode Bound or Packing bound **[Etzion-Vardy** IEEE TIT, **2011–Frankl-Wilson** JCTA, **1986]**

$$A_q(n,d;k) \leq \frac{|\mathcal{G}_q(n,k)|}{|\mathcal{A}_{n,k}(Y;\delta-1)|} = \frac{\begin{bmatrix} n \\ k \end{bmatrix}_q}{\begin{bmatrix} n-k+\delta-1 \\ \delta-1 \end{bmatrix}_q} = \frac{\begin{bmatrix} n \\ k-\delta+1 \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\delta+1 \end{bmatrix}_q}$$

$\mathcal{A}_{n,k}(Y;\delta-1) = \{W \in \mathcal{G}_q(n,k) \, : \, Y \subseteq W\}$ for $Y \in \mathcal{G}_q(n,k-\delta+1)$
anticode of diameter $\delta - 1$ in $\mathcal{G}_q(n,k)$ of largest possible size

$$\mathcal{P} = \{(Y,W) \, : \, Y \in \mathcal{G}_q(n,k-\delta+1),\ W \in \mathcal{C} \, : \, Y \subseteq W\}$$

Anticode Bound

$$A_q(n,d;k),\ d=2\delta \text{ and } k\le \tfrac{n}{2}$$

Anticode Bound or Packing bound **[Etzion-Vardy** IEEE TIT, **2011–Frankl-Wilson** JCTA, **1986]**

$$A_q(n,d;k)\le \frac{|\mathcal{G}_q(n,k)|}{|\mathcal{A}_{n,k}(Y;\delta-1)|}=\frac{\begin{bmatrix}n\\k\end{bmatrix}_q}{\begin{bmatrix}n-k+\delta-1\\ \delta-1\end{bmatrix}_q}=\frac{\begin{bmatrix}n\\k-\delta+1\end{bmatrix}_q}{\begin{bmatrix}k\\k-\delta+1\end{bmatrix}_q}$$

$\mathcal{A}_{n,k}(Y;\delta-1)=\{W\in\mathcal{G}_q(n,k)\ :\ Y\subseteq W\}$ for $Y\in\mathcal{G}_q(n,k-\delta+1)$
anticode of diameter $\delta-1$ in $\mathcal{G}_q(n,k)$ of largest possible size

$$\mathcal{P}=\{(Y,W)\ :\ Y\in\mathcal{G}_q(n,k-\delta+1),\ W\in\mathcal{C}\ :\ Y\subseteq W\}$$

S. Kurz: *Constructions and bound for subspace codes*, arXiv, **2025**.

Anticode Bound

$$A_q(n,d;k),\ d=2\delta \text{ and } k\leq \tfrac{n}{2}$$

Anticode Bound or Packing bound **[Etzion-Vardy** IEEE TIT, **2011–Frankl-Wilson** JCTA, **1986]**

$$A_q(n,d;k)\leq \frac{|\mathcal{G}_q(n,k)|}{|\mathcal{A}_{n,k}(Y;\delta-1)|}=\frac{\begin{bmatrix} n\\ k\end{bmatrix}_q}{\begin{bmatrix} n-k+\delta-1\\ \delta-1\end{bmatrix}_q}=\frac{\begin{bmatrix} n\\ k-\delta+1\end{bmatrix}_q}{\begin{bmatrix} k\\ k-\delta+1\end{bmatrix}_q}$$

$\mathcal{A}_{n,k}(Y;\delta-1)=\{W\in\mathcal{G}_q(n,k)\ :\ Y\subseteq W\}$ for $Y\in\mathcal{G}_q(n,k-\delta+1)$
anticode of diameter $\delta-1$ in $\mathcal{G}_q(n,k)$ of largest possible size

$$\mathcal{P}=\{(Y,W)\ :\ Y\in\mathcal{G}_q(n,k-\delta+1),\ W\in\mathcal{C}\ :\ Y\subseteq W\}$$

$A_q(n,d,k)$ **for** $n\to\infty$ **[Blackburn-Etzion** IEEE TIT, **2012]**

Let q, k, and $d=2\delta$ be fixed integers with $0\leq\delta\leq k+1$ and such that q is a prime power. Then

$$A_q(n,d,k)\sim\frac{\begin{bmatrix} n\\ k-\delta+1\end{bmatrix}_q}{\begin{bmatrix} k\\ k-\delta+1\end{bmatrix}_q}\qquad n\to\infty$$

Optimal Subspace Codes

$$A_q(n,d;k) \stackrel{?}{=} \frac{\begin{bmatrix} n \\ k-\frac{d}{2}+1 \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\frac{d}{2}+1 \end{bmatrix}_q}$$

Optimal Subspace Codes

$$A_q(n,d;k) \stackrel{?}{=} \frac{\begin{bmatrix} n \\ k-\frac{d}{2}+1 \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\frac{d}{2}+1 \end{bmatrix}_q}$$

Spread Codes

$$d = 2k$$

Optimal Subspace Codes

$$A_q(n,d;k) \stackrel{?}{=} \frac{\begin{bmatrix} n \\ k-\frac{d}{2}+1 \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\frac{d}{2}+1 \end{bmatrix}_q}$$

Spread Codes

$$d = 2k \implies A_q(n, d = 2k, k) \leq \frac{\begin{bmatrix} n \\ 1 \end{bmatrix}_q}{\begin{bmatrix} k \\ 1 \end{bmatrix}_q} = \frac{q^n - 1}{q^k - 1}$$

Optimal Subspace Codes

$$A_q(n,d;k) \overset{?}{=} \frac{\begin{bmatrix} n \\ k-\frac{d}{2}+1 \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\frac{d}{2}+1 \end{bmatrix}_q}$$

Spread Codes

$$d = 2k \implies A_q(n, d = 2k, k) \leq \frac{\begin{bmatrix} n \\ 1 \end{bmatrix}_q}{\begin{bmatrix} k \\ 1 \end{bmatrix}_q} = \frac{q^n-1}{q^k-1}$$

$$A_q(n, d = 2k, k) = \frac{q^n-1}{q^k-1}$$

Optimal Subspace Codes

$$A_q(n,d;k) \overset{?}{=} \frac{\begin{bmatrix} n \\ k-\frac{d}{2}+1 \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\frac{d}{2}+1 \end{bmatrix}_q}$$

Spread Codes

$$d = 2k \implies A_q(n, d = 2k, k) \leq \frac{\begin{bmatrix} n \\ 1 \end{bmatrix}_q}{\begin{bmatrix} k \\ 1 \end{bmatrix}_q} = \frac{q^n - 1}{q^k - 1}$$

$$A_q(n, d = 2k, k) = \frac{q^n - 1}{q^k - 1} \implies k \mid n.$$

Optimal Subspace Codes

$$A_q(n,d;k) \stackrel{?}{=} \frac{\begin{bmatrix} n \\ k-\frac{d}{2}+1 \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\frac{d}{2}+1 \end{bmatrix}_q}$$

Spread Codes

$$d=2k \implies A_q(n,d=2k,k) \leq \frac{\begin{bmatrix} n \\ 1 \end{bmatrix}_q}{\begin{bmatrix} k \\ 1 \end{bmatrix}_q} = \frac{q^n-1}{q^k-1}$$

$$A_q(n,d=2k,k) = \frac{q^n-1}{q^k-1} \implies k \mid n.$$

$\mathcal{S} \subseteq \mathcal{G}_q(kr,k)$ with parameters $(n=kr, d=2k, \frac{q^{kr}-1}{q^k-1})_q$ is a *spread code*

Spreads of projective spaces $\longrightarrow$ translation structures

B. Segre: *Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane*
ANNALI DI MATEMATUCA PURA E APPLICATA, **1964**.

Spreads of projective spaces $\longrightarrow$ translation structures

B. Segre: *Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane*
ANNALI DI MATEMATUCA PURA E APPLICATA, **1964**.

There exist spread codes $\forall\, q$ and $\forall k$ such that $k \mid n$

$$A_q(n, d = 2k, k) = \frac{q^n - 1}{q^k - 1}$$

Spreads of projective spaces $\longrightarrow$ translation structures

B. Segre: *Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane* ANNALI DI MATEMATUCA PURA E APPLICATA, **1964**.

There exist spread codes $\forall\, q$ and $\forall k$ such that $k \mid n$

$$A_q(n, d = 2k, k) = \frac{q^n - 1}{q^k - 1}$$

A. Barlotti, J. Cofman: *Finite Sperner spaces constructed from projective and affine spaces.* ABH. MATH. SEM. UNIV. HAMBURG, **1974**.

Spreads of projective spaces $\longrightarrow$ translation structures

B. Segre: *Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane* ANNALI DI MATEMATUCA PURA E APPLICATA, **1964**.

There exist spread codes $\forall\, q$ and $\forall k$ such that $k \mid n$

$$A_q(n, d = 2k, k) = \frac{q^n - 1}{q^k - 1}$$

A. Barlotti, J. Cofman: *Finite Sperner spaces constructed from projective and affine spaces.* ABH. MATH. SEM. UNIV. HAMBURG, **1974**.

$n = 2k$

Spreads of projective spaces $\longrightarrow$ translation structures

B. Segre: *Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane* ANNALI DI MATEMATUCA PURA E APPLICATA, **1964**.

There exist spread codes $\forall\, q$ and $\forall k$ such that $k \mid n$

$$A_q(n, d = 2k, k) = \frac{q^n - 1}{q^k - 1}$$

A. Barlotti, J. Cofman: *Finite Sperner spaces constructed from projective and affine spaces.* ABH. MATH. SEM. UNIV. HAMBURG, **1974**.

$n = 2k \quad \longrightarrow$ *planar spread*

Spreads of projective spaces $\longrightarrow$ translation structures

B. Segre: *Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane* ANNALI DI MATEMATUCA PURA E APPLICATA, **1964**.

There exist spread codes $\forall\, q$ and $\forall k$ such that $k \mid n$

$$A_q(n, d = 2k, k) = \frac{q^n - 1}{q^k - 1}$$

A. Barlotti, J. Cofman: *Finite Sperner spaces constructed from projective and affine spaces.* ABH. MATH. SEM. UNIV. HAMBURG, **1974**.

$n = 2k \quad \longrightarrow$ *planar spread* $\longleftrightarrow$ *translation plane*

Spreads of projective spaces $\longrightarrow$ translation structures

B. Segre: *Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane* ANNALI DI MATEMATUCA PURA E APPLICATA, **1964**.

There exist spread codes $\forall\, q$ and $\forall k$ such that $k \mid n$

$$A_q(n, d = 2k, k) = \frac{q^n - 1}{q^k - 1}$$

A. Barlotti, J. Cofman: *Finite Sperner spaces constructed from projective and affine spaces.* ABH. MATH. SEM. UNIV. HAMBURG, **1974**.

$n = 2k \quad \longrightarrow$ *planar spread* $\longleftrightarrow$ *translation plane* $\longleftarrow$ *semifields*

Spreads of projective spaces $\longrightarrow$ translation structures

B. Segre: *Teoria di Galois, fibrazioni proiettive e geometrie non desarguesiane* ANNALI DI MATEMATUCA PURA E APPLICATA, **1964**.

There exist spread codes $\forall\, q$ and $\forall k$ such that $k \mid n$

$$A_q(n, d = 2k, k) = \frac{q^n - 1}{q^k - 1}$$

A. Barlotti, J. Cofman: *Finite Sperner spaces constructed from projective and affine spaces.* ABH. MATH. SEM. UNIV. HAMBURG, **1974**.

$n = 2k \;\longrightarrow$ *planar spread* $\longleftrightarrow$ *translation plane* $\longleftarrow$ *semifields*

J. André: *Über nicht-Desarguessche Ebenen mit transitive Translationgruppe.* MATH. Z., **1954**.

R.H. Bruck, R.C. Bose: *The construction of translation planes from projective spaces* J. ALGEBRA, **1964**.

H. Lübeburg: *Translation Planes,* BERLIN: SPRINGER VERLAG, **1980**.

M. Biliotti, V. Jha, N. L. Johnson: *Foundations of Translation Planes,* MARCEL DEKKER, **2001**.

G. Lunardon: *50 Years of translation structures,* JOURNAL OF GEOMETRY, **2022**.

q-Steiner systems

$$A_q(n, d = 2\delta; k) \overset{?}{=} \frac{\begin{bmatrix} n \\ k-\delta+1 \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\delta+1 \end{bmatrix}_q}$$

q-Steiner systems

$$A_q(n, d = 2\delta; k) \stackrel{?}{=} \frac{\begin{bmatrix} n \\ k-\delta+1 \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\delta+1 \end{bmatrix}_q}$$

$$t := k - \delta + 1$$

q-Steiner systems

$$A_q(n, d = 2\delta; k) \stackrel{?}{=} \frac{\begin{bmatrix} n \\ k-\delta+1 \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\delta+1 \end{bmatrix}_q} = \frac{\begin{bmatrix} n \\ t \end{bmatrix}_q}{\begin{bmatrix} k \\ t \end{bmatrix}_q}$$

$$t := k - \delta + 1$$

q-Steiner system

$\mathcal{S} \subseteq \mathcal{G}_q(n, k)$ with parameters $(n, d = 2(k - t + 1), M)_q$ with $M = \frac{\begin{bmatrix} n \\ t \end{bmatrix}_q}{\begin{bmatrix} k \\ t \end{bmatrix}_q}$

$\mathcal{S} = \mathcal{S}_q(t, k, n)$ is a q-Steiner system

q-Steiner systems

$$A_q(n, d = 2\delta; k) \stackrel{?}{=} \frac{\begin{bmatrix} n \\ k-\delta+1 \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\delta+1 \end{bmatrix}_q} = \frac{\begin{bmatrix} n \\ t \end{bmatrix}_q}{\begin{bmatrix} k \\ t \end{bmatrix}_q}$$

$$t := k - \delta + 1$$

q-Steiner system

$\mathcal{S} \subseteq \mathcal{G}_q(n,k)$ with parameters $(n, d = 2(k-t+1), M)_q$ with $M = \frac{\begin{bmatrix} n \\ t \end{bmatrix}_q}{\begin{bmatrix} k \\ t \end{bmatrix}_q}$

$\mathcal{S} = \mathcal{S}_q(t,k,n)$ is a q-Steiner system

$$\mathcal{P} = \{(Y, W) \,:\, Y \in \mathcal{G}_q(n,t),\ W \in \mathcal{S} \,:\, Y \subseteq W\}$$

q-Steiner systems

$$A_q(n, d = 2\delta; k) \stackrel{?}{=} \frac{\begin{bmatrix} n \\ k-\delta+1 \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\delta+1 \end{bmatrix}_q} = \frac{\begin{bmatrix} n \\ t \end{bmatrix}_q}{\begin{bmatrix} k \\ t \end{bmatrix}_q}$$

$$t := k - \delta + 1$$

q-Steiner system

$$\mathcal{S} \subseteq \mathcal{G}_q(n,k) \text{ with parameters } (n, d = 2(k-t+1), M)_q \text{ with } M = \frac{\begin{bmatrix} n \\ t \end{bmatrix}_q}{\begin{bmatrix} k \\ t \end{bmatrix}_q}$$

$\mathcal{S} = \mathcal{S}_q(t,k,n)$ is a q-Steiner system

$$\Updownarrow$$

$$\forall Y \in \mathcal{G}_q(n,t)\ \exists! W \in \mathcal{S} \ :\ \ Y \subseteq W.$$

$$\mathcal{P} = \{(Y, W) \ :\ Y \in \mathcal{G}_q(n,t),\ W \in \mathcal{S} \ :\ Y \subseteq W\}$$

q-Steiner systems

$$A_q(n, d = 2\delta; k) \stackrel{?}{=} \frac{\begin{bmatrix} n \\ k-\delta+1 \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\delta+1 \end{bmatrix}_q} = \frac{\begin{bmatrix} n \\ t \end{bmatrix}_q}{\begin{bmatrix} k \\ t \end{bmatrix}_q}$$

$t := k - \delta + 1$ $\quad$ $t = 1$ spread codes

q-Steiner system

$\mathcal{S} \subseteq \mathcal{G}_q(n,k)$ with parameters $(n, d = 2(k-t+1), M)_q$ with $M = \frac{\begin{bmatrix} n \\ t \end{bmatrix}_q}{\begin{bmatrix} k \\ t \end{bmatrix}_q}$

$\mathcal{S} = \mathcal{S}_q(t,k,n)$ is a q-Steiner system

$$\Updownarrow$$

$$\forall Y \in \mathcal{G}_q(n,t)\ \exists! W \in \mathcal{S} \ :\ \ Y \subseteq W.$$

$$\mathcal{P} = \{(Y, W)\ :\ Y \in \mathcal{G}_q(n,t),\ W \in \mathcal{S}\ :\ Y \subseteq W\}$$

q-Steiner systems

$$A_q(n, d = 2\delta; k) \overset{?}{=} \frac{\begin{bmatrix} n \\ k-\delta+1 \end{bmatrix}_q}{\begin{bmatrix} k \\ k-\delta+1 \end{bmatrix}_q} = \frac{\begin{bmatrix} n \\ t \end{bmatrix}_q}{\begin{bmatrix} k \\ t \end{bmatrix}_q}$$

$t := k - \delta + 1$ $\quad t = 1$ spread codes

q-Steiner system

$$\mathcal{S} \subseteq \mathcal{G}_q(n, k) \text{ with parameters } (n, d = 2(k - t + 1), M)_q \text{ with } M = \frac{\begin{bmatrix} n \\ t \end{bmatrix}_q}{\begin{bmatrix} k \\ t \end{bmatrix}_q}$$

$\mathcal{S} = \mathcal{S}_q(t, k, n)$ is a q-Steiner system

$$\Updownarrow$$

$$\forall Y \in \mathcal{G}_q(n, t)\ \exists! W \in \mathcal{S} \ : \ Y \subseteq W.$$

$$\mathcal{P} = \{(Y, W) \ : \ Y \in \mathcal{G}_q(n, t),\ W \in \mathcal{S} \ : \ Y \subseteq W\}$$

M. Schwartz, T. Etzion: *Codes and Anticodes in the Grassman Graph*, JCTA, **2002**.

q-Steiner systems: known examples

$t, k, n, q \in \mathbb{N}$, $t \leq k \leq n$, q a prime power

q-Steiner systems: known examples

$t, k, n, q \in \mathbb{N}$, $t \leq k \leq n$, q a prime power

$\mathcal{S}_q(t, n, n)$ exists for each q
$\mathcal{S}_q(k, k, n)$ exists for each q

q-Steiner systems: known examples

$t, k, n, q \in \mathbb{N}$, $t \leq k \leq n$, q a prime power

$\mathcal{S}_q(t, n, n)$ exists for each q
$\mathcal{S}_q(k, k, n)$ exists for each q

$\mathcal{S}_q(1, k, rk)$ exists for each q, spread codes

q-Steiner systems: known examples

$t, k, n, q \in \mathbb{N}$, $t \leq k \leq n$, q a prime power

$\mathcal{S}_q(t, n, n)$ exists for each q
$\mathcal{S}_q(k, k, n)$ exists for each q

$\mathcal{S}_q(1, k, rk)$ exists for each q, spread codes

$\mathcal{S}_q(t, k, n)$ with $t \geq 2$ and $t < k < n$

q-Steiner systems: known examples

$t, k, n, q \in \mathbb{N}$, $t \leq k \leq n$, q a prime power

$\mathcal{S}_q(t, n, n)$ exists for each q
$\mathcal{S}_q(k, k, n)$ exists for each q

$\mathcal{S}_q(1, k, rk)$ exists for each q, spread codes

$\mathcal{S}_q(t, k, n)$ with $t \geq 2$ and $t < k < n$ **OPEN PROBLEM**

q-Steiner systems: known examples

$t, k, n, q \in \mathbb{N}$, $t \leq k \leq n$, q a prime power

$\mathcal{S}_q(t, n, n)$ exists for each q
$\mathcal{S}_q(k, k, n)$ exists for each q

$\mathcal{S}_q(1, k, rk)$ exists for each q, spread codes

$\mathcal{S}_q(t, k, n)$ with $t \geq 2$ and $t < k < n$ **OPEN PROBLEM**

A. Beutelspacher: *Parallelismen in unendlichen projektiven Raumen endlicher Dimension*, GEOMETRIAE DEDICATA, **1978**.

q-Steiner systems: known examples

$t, k, n, q \in \mathbb{N}$, $t \leq k \leq n$, q a prime power

$\mathcal{S}_q(t, n, n)$ exists for each q
$\mathcal{S}_q(k, k, n)$ exists for each q

$\mathcal{S}_q(1, k, rk)$ exists for each q, spread codes

$\mathcal{S}_q(t, k, n)$ with $t \geq 2$ and $t < k < n$ **OPEN PROBLEM**

There exist $\mathcal{S}_2(2, 3, 13)$ 2-systems $\longleftrightarrow$ $A_2(13, 4, 3) = \dfrac{\begin{bmatrix} 13 \\ 2 \end{bmatrix}_2}{\begin{bmatrix} 3 \\ 2 \end{bmatrix}_2} = 1597245$

M. Braun, T. Etzion, P. Östergård, A. Vardy, A. Wassermann: *Existence of q-analogs of steiner systems,* Forum of Mathematics, Pi, **2016**.

q-Steiner systems: known examples

$t, k, n, q \in \mathbb{N}$, $t \leq k \leq n$, q a prime power

$\mathcal{S}_q(t, n, n)$ exists for each q
$\mathcal{S}_q(k, k, n)$ exists for each q

$\mathcal{S}_q(1, k, rk)$ exists for each q, spread codes

$\mathcal{S}_q(t, k, n)$ with $t \geq 2$ and $t < k < n$ **OPEN PROBLEM**

There exist $\mathcal{S}_2(2, 3, 13)$ 2-systems $\longleftrightarrow$ $A_2(13, 4, 3) = \dfrac{\begin{bmatrix} 13 \\ 2 \end{bmatrix}_2}{\begin{bmatrix} 3 \\ 2 \end{bmatrix}_2} = 1597245$

M. Braun, T. Etzion, P. Östergård, A. Vardy, A. Wassermann: *Existence of q-analogs of steiner systems*, Forum of Mathematics, Pi, **2016**.

$Aut(\mathcal{S}_2(2, 3, 13))$ contains the normalizer of a Singer subgroup of $GL(13, 2)$

Cyclic subspace codes in $\mathbb{V}(n, q)$

T. Etzion and A. Vardy : *Error-correcting codes in projective space*, IEEE Transaction on Information Theory, **2011**.

Cyclic subspace codes in $\mathbb{V}(n, q)$

T. Etzion and A. Vardy : *Error-correcting codes in projective space,* IEEE TRANSACTION ON INFORMATION THEORY, **2011**.

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

Cyclic subspace codes in $\mathbb{V}(n, q)$

T. Etzion and A. Vardy : *Error-correcting codes in projective space*, IEEE TRANSACTION ON INFORMATION THEORY, **2011**.

$$\mathcal{C} \subseteq \mathcal{G}_q(n, k) \text{ is cyclic}$$

$$\text{if } \exists \text{ a Singer subgroup } G \leq GL(n, k) \ : \ G \leq Aut(\mathcal{C})$$

Cyclic subspace codes in $\mathbb{V}(n, q)$

T. Etzion and A. Vardy : *Error-correcting codes in projective space,* IEEE TRANSACTION ON INFORMATION THEORY, **2011**.

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

if $\exists$ a Singer subgroup $G \leq GL(n, k)$: $G \leq Aut(\mathcal{C})$

$$\forall \varphi \in G \text{ and } \forall V \in \mathcal{C} \quad \Longrightarrow \quad \varphi(V) \in \mathcal{C}$$

Cyclic subspace codes in $\mathbb{V}(n, q)$

T. Etzion and A. Vardy : *Error-correcting codes in projective space,* IEEE Transaction on Information Theory, **2011**.

$$\mathcal{C} \subseteq \mathcal{G}_q(n, k) \text{ is cyclic}$$

$$\text{if } \exists \text{ a Singer subgroup } G \leq GL(n, k) \ : \ G \leq Aut(\mathcal{C})$$

$$\forall \varphi \in G \text{ and } \forall V \in \mathcal{C} \quad \Longrightarrow \quad \varphi(V) \in \mathcal{C}$$

$$\Updownarrow$$

$$\mathcal{C} = \cup_V Orb_G(V) = \cup_V \{\varphi(V) \ : \ \varphi \in G\}$$

Cyclic orbit codes

$\mathcal{C} = Orb_G(V) \subseteq \mathcal{G}_q(n, k)$ cyclic orbit code

Cyclic orbit codes

$$\mathcal{C} = Orb_G(V) \subseteq \mathcal{G}_q(n,k) \quad \text{cyclic orbit code}$$

$$d(\varphi(V), \psi(V)) = d(V, \varphi^{-1}(\psi(V)) \quad \forall \varphi, \psi \in G$$

Cyclic orbit codes

$$\mathcal{C} = Orb_G(V) \subseteq \mathcal{G}_q(n,k) \quad \text{cyclic orbit code}$$

$$d(\varphi(V), \psi(V)) = d(V, \varphi^{-1}(\psi(V)) \quad \forall \varphi, \psi \in G$$

$$\mathcal{C} = Orb_G(V) \quad (n, d, |\mathcal{C}|, k)_q$$

$$d = \min\{d(V, \varphi(V)) \ : \ \varphi \in G, \varphi(V) \neq V\}$$

Cyclic orbit codes

$$\mathcal{C} = Orb_G(V) \subseteq \mathcal{G}_q(n,k) \quad \text{cyclic orbit code}$$

$$d(\varphi(V), \psi(V)) = d(V, \varphi^{-1}(\psi(V)) \quad \forall \varphi, \psi \in G$$

$$\mathcal{C} = Orb_G(V) \quad (n, d, |\mathcal{C}|, k)_q$$

$$d = \min\{d(V, \varphi(V)) \, : \, \varphi \in G, \varphi(V) \neq V\}$$

$$\omega(\mathcal{C}) = (\omega_d(\mathcal{C}), \omega_{d+2}(\mathcal{C}), \ldots\ldots, \omega_{2k}(\mathcal{C})) \quad \text{distance distribution of } \mathcal{C}$$

$$\omega_{2i}(\mathcal{C}) = |\{\varphi(V) \in Orb_G(V) \, : \, d(V, \varphi(V)) = 2i\}|$$

Cyclic orbit codes

$$\mathcal{C} = Orb_G(V) \quad (n, d, |\mathcal{C}|, k)_q, \; d \in \{2, 4, ..., 2k-4, 2k-2, 2k\}$$

Cyclic orbit codes

$$\mathcal{C} = Orb_G(V) \quad (n, d, |\mathcal{C}|, k)_q, \; d \in \{2, 4, ..., 2k-4, 2k-2, 2k\}$$

Cyclic orbit codes

$$\mathcal{C} = Orb_G(V) \quad (n, d, |\mathcal{C}|, k)_q,\; d \in \{2, 4, ..., 2k-4, 2k-2, 2k\}$$

$$|\mathcal{C}| \leq \frac{q^n-1}{q-1}$$

Cyclic orbit codes

$$\mathcal{C} = Orb_G(V) \quad (n, d, |\mathcal{C}|, k)_q,\ d \in \{2, 4, \ldots\ldots, 2k-4, 2k-2, 2k\}$$

$$|\mathcal{C}| \leq \frac{q^n-1}{q-1}$$

$$|\mathcal{C}| = \frac{q^n-1}{q-1} \longrightarrow \text{full-length orbit code}$$

Cyclic orbit codes

$$\mathcal{C} = Orb_G(V) \quad (n, d, |\mathcal{C}|, k)_q, \; d \in \{2, 4, ..., 2k-4, 2k-2, 2k\}$$

$$|\mathcal{C}| \leq \frac{q^n-1}{q-1}$$

$|\mathcal{C}| = \frac{q^n-1}{q-1} \longrightarrow$ full-length orbit code

$$d = 2k \quad \Longrightarrow |\mathcal{C}| < \frac{q^n-1}{q-1}$$

Cyclic orbit codes

$$\mathcal{C} = Orb_G(V) \quad (n, d, |\mathcal{C}|, k)_q, \; d \in \{2, 4, ..., 2k-4, 2k-2, 2k\}$$

$$|\mathcal{C}| \leq \frac{q^n-1}{q-1}$$

$|\mathcal{C}| = \frac{q^n-1}{q-1} \longrightarrow$ full-length orbit code

$$d = 2k \quad \Longrightarrow |\mathcal{C}| < \frac{q^n-1}{q-1}$$

Cyclic orbit codes

$$\mathcal{C} = Orb_G(V) \quad (n, d, |\mathcal{C}|, k)_q,\ d \in \{2, 4, ..., 2k-4, 2k-2, 2k\}$$

$$|\mathcal{C}| \leq \frac{q^n-1}{q-1}$$

$|\mathcal{C}| = \frac{q^n-1}{q-1} \longrightarrow$ full-length orbit code

$$d = 2k \quad \Longrightarrow |\mathcal{C}| < \frac{q^n-1}{q-1}$$

$\mathcal{C} = Orb_G(V) \quad (n, 2k-2, \frac{q^n-1}{q-1})_q$

Cyclic orbit codes

$$\mathcal{C} = Orb_G(V) \quad (n, d, |\mathcal{C}|, k)_q,\ d \in \{2, 4, \ldots\ldots, 2k-4, 2k-2, 2k\}$$

$$|\mathcal{C}| \leq \frac{q^n-1}{q-1}$$

$$|\mathcal{C}| = \frac{q^n-1}{q-1} \longrightarrow \text{full-length orbit code}$$

$$d = 2k \quad \Longrightarrow |\mathcal{C}| < \frac{q^n-1}{q-1}$$

Optimal cyclic orbit code

$$\mathcal{C} = Orb_G(V) \quad (n, 2k-2, \tfrac{q^n-1}{q-1})_q$$

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

Cyclic orbit codes

$$\mathcal{C} = Orb_G(V) \quad (n, d, |\mathcal{C}|, k)_q, \; d \in \{2, 4, \ldots\ldots, 2k-4, 2k-2, 2k\}$$

$$|\mathcal{C}| \leq \frac{q^n-1}{q-1}$$

$$|\mathcal{C}| = \frac{q^n-1}{q-1} \longrightarrow \text{full-length orbit code}$$

$$d = 2k \quad \Longrightarrow |\mathcal{C}| < \frac{q^n-1}{q-1}$$

Optimal cyclic orbit code

$$\mathcal{C} = Orb_G(V) \quad (n, 2k-2, \tfrac{q^n-1}{q-1})_q$$

Quasi-optimal cyclic orbit code

$$\mathcal{C} = Orb_G(V) \quad (n, 2k-4, \tfrac{q^n-1}{q-1})_q$$

A.-L. Trautmann, F. Manganiello, M. Braun and J. Rosenthal: *Cyclic orbit codes*, IEEE TRANSACTION ON INFORMATION THEORY, **2013**.

Cyclic orbit codes

$$\mathcal{C} = Orb_G(V) \quad (n, d, |\mathcal{C}|, k)_q,\; d \in \{2, 4, ..., 2k-4, 2k-2, 2k\}$$

$$|\mathcal{C}| \leq \frac{q^n-1}{q-1}$$

$$|\mathcal{C}| = \frac{q^n-1}{q-1} \longrightarrow$$ full-length orbit code

$$d = 2k \quad \Longrightarrow |\mathcal{C}| < \frac{q^n-1}{q-1}$$

Optimal cyclic orbit code

$$\mathcal{C} = Orb_G(V) \quad (n, 2k-2, \tfrac{q^n-1}{q-1})_q$$

Quasi-optimal cyclic orbit code

$$\mathcal{C} = Orb_G(V) \quad (n, 2k-4, \tfrac{q^n-1}{q-1})_q$$

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

H. Gluesing-Luerssen and H. Lehmann: *Distance distributions of cyclic orbit codes,* Designs, Codes and Cryptography, **2021**.

Cyclic subspace codes in $\mathbb{F}_{q^n}$

$$\mathbb{V}(n,q) \equiv \mathbb{F}_{q^n}$$

Cyclic subspace codes in $\mathbb{F}_{q^n}$

$$\mathbb{V}(n,q) \equiv \mathbb{F}_{q^n}$$

$$\varphi_\alpha \,:\, x \in \mathbb{F}_{q^n} \mapsto \alpha x \in \mathbb{F}_{q^n} \quad \alpha \in \mathbb{F}_{q^n}^*$$

$$G = \{\varphi_\alpha \,:\, \alpha \in \mathbb{F}_{q^n}^*\} \cong \mathbb{F}_{q^n}^* \text{ Singer cycle}$$

Cyclic subspace codes in $\mathbb{F}_{q^n}$

$$\mathbb{V}(n,q) \equiv \mathbb{F}_{q^n}$$

$$\varphi_\alpha \ : \ x \in \mathbb{F}_{q^n} \mapsto \alpha x \in \mathbb{F}_{q^n} \quad \alpha \in \mathbb{F}_{q^n}^*$$

$$G = \{\varphi_\alpha \ : \ \alpha \in \mathbb{F}_{q^n}^*\} \cong \mathbb{F}_{q^n}^* \text{ Singer cycle}$$

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

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

Cyclic subspace codes in $\mathbb{F}_{q^n}$

$$\mathbb{V}(n,q) \equiv \mathbb{F}_{q^n}$$

$$\varphi_\alpha \,:\, x \in \mathbb{F}_{q^n} \mapsto \alpha x \in \mathbb{F}_{q^n} \quad \alpha \in \mathbb{F}_{q^n}^*$$

$$G = \{\varphi_\alpha \,:\, \alpha \in \mathbb{F}_{q^n}^*\} \cong \mathbb{F}_{q^n}^* \text{ Singer cycle}$$

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

$$\forall \alpha \in \mathbb{F}_{q^n}^* \text{ and } \forall V \in \mathcal{C} \implies \alpha V \in \mathcal{C}$$

$$\alpha V = \{\alpha \cdot v \,:\, v \in V\} \quad \text{a cyclic shift of } V$$

Cyclic subspace codes in $\mathbb{F}_{q^n}$

$$\mathbb{V}(n,q) \equiv \mathbb{F}_{q^n}$$

$$\varphi_\alpha \,:\, x \in \mathbb{F}_{q^n} \mapsto \alpha x \in \mathbb{F}_{q^n} \quad \alpha \in \mathbb{F}_{q^n}^*$$

$$G = \{\varphi_\alpha \,:\, \alpha \in \mathbb{F}_{q^n}^*\} \cong \mathbb{F}_{q^n}^* \text{ Singer cycle}$$

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

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

$$\alpha V = \{\alpha \cdot v \,:\, v \in V\} \quad \text{a cyclic shift of } V$$

$$\mathcal{C} = \mathrm{Orb}_{\mathbb{F}_{q^n}^*}(V) = \{\alpha V \,:\, \alpha \in \mathbb{F}_{q^n}^*\} \text{ cyclic orbit code}$$

Cyclic subspace codes in $\mathbb{F}_{q^n}$

$$V \in \mathcal{G}_q(n,k): \quad k\text{-dimensional } \mathbb{F}_q\text{-subspaces of } \mathbb{F}_{q^n}$$

Cyclic subspace codes in $\mathbb{F}_{q^n}$

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

$\mathcal{C} = \mathrm{Orb}(V) := \mathrm{Orb}_{\mathbb{F}_{q^n}^*}(V)$ cyclic orbit code

Cyclic subspace codes in $\mathbb{F}_{q^n}$

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

$$\mathcal{C} = \mathrm{Orb}(V) := \mathrm{Orb}_{\mathbb{F}_{q^n}^*}(V) \quad \text{cyclic orbit code}$$

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

Cyclic subspace codes in $\mathbb{F}_{q^n}$

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

$$\mathcal{C} = \mathrm{Orb}(V) := \mathrm{Orb}_{\mathbb{F}^*_{q^n}}(V) \quad \text{cyclic orbit code}$$

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

$$s := \max\{t \mid n : V \text{ is } \mathbb{F}_{q^t} - linear\}$$

Cyclic subspace codes in $\mathbb{F}_{q^n}$

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

$$\mathcal{C} = \mathrm{Orb}(V) := \mathrm{Orb}_{\mathbb{F}_{q^n}^*}(V) \quad \text{cyclic orbit code}$$

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

$$s := \max\{t \mid n : V \text{ is } \mathbb{F}_{q^t} - linear\}$$

Cyclic subspace codes in $\mathbb{F}_{q^n}$

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

$$\mathcal{C} = \mathrm{Orb}(V) := \mathrm{Orb}_{\mathbb{F}_{q^n}^*}(V) \quad \text{cyclic orbit code}$$

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

$$s := \max\{t \mid n \ : \ V \ \text{ is } \ \mathbb{F}_{q^t} - linear\}$$

$$l := \max\{\dim(V \cap \alpha V) \ : \ \alpha \in \mathbb{F}_{q^n}^*, \alpha V \neq V\}$$

Desarguesian spread codes

$$\mathcal{C} = \mathrm{Orb}(V) := \mathrm{Orb}_{\mathbb{F}_{q^n}^*}(V) \quad \text{cyclic orbit code}$$

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

$$\omega(\mathcal{C}) = (\omega_{2k}(\mathcal{C})) = (\frac{q^n-1}{q^k-1} - 1)$$

$$s = k\,|\,n\,,\, \mathcal{C} = Orb(\mathbb{F}_{q^k}) \longrightarrow [n, 2k, \frac{q^n-1}{q^k-1}, k]_q$$

Desarguesian spread code

Desarguesian spread codes

$$\mathcal{C} = \mathrm{Orb}(V) := \mathrm{Orb}_{\mathbb{F}_{q^n}^*}(V) \quad \text{cyclic orbit code}$$

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

$$\omega(\mathcal{C}) = (\omega_{2k}(\mathcal{C})) = (\frac{q^n-1}{q^k-1} - 1)$$

$$s = k \,|\, n, \mathcal{C} = Orb(\mathbb{F}_{q^k}) \longrightarrow [n, 2k, \frac{q^n-1}{q^k-1}, k]_q$$

Desarguesian spread code

F. Manganiello, E. Gorla, J. Rosenthal *Spread Codes and Spread Decoding in Network Coding,* IEEE TIT, **2013**.

E. Gorla, F. Manganiello: *An Algebraic Approach for Decoding Spread Codes* Advances in Mathematics of Communications , **2011**.

E. Franch, C. Li, A. Piccirillo: *Decoding Desarguesian spread codes beyond half minimum distance* Man,**2026**.

Recent results on cyclic subspace codes

GGA

Galois geometries and their applications

Recent results on cyclic subspace codes

GGA

Galois geometries and their applications

C. Castello, O.P., F. Zullo: *On one-orbit cyclic subspace codes of $\mathcal{G}_q(n,3)$* , IEEE, ISIT PROCEEDINGS, **2024**.

C. Castello, O.P., F. Zullo: *Full weight spectrum one-orbit cyclic subspace codes*, J. COMB. THEORY, S. A, **2025**.

C. Castello, A. Couvreur, O.P., F. Zullo : *Subspaces of finite field extensions with small square-span*, ONGOING PROJECT.

Recent results on cyclic subspace codes

GGA

Galois geometries and their applications

- **C. Castello, O.P., F. Zullo:** *On one-orbit cyclic subspace codes of $\mathcal{G}_q(n,3)$* , IEEE, ISIT PROCEEDINGS, **2024**.
- **C. Castello, O.P., F. Zullo:** *Full weight spectrum one-orbit cyclic subspace codes*, J. COMB. THEORY, S. A, **2025**.
- **C. Castello, A. Couvreur, O.P., F. Zullo :** *Subspaces of finite field extensions with small square-span*, ONGOING PROJECT.
- **C. Castello, O.P., P. Santonastaso. F. Zullo:** *Construction and equivalence of Sidon sapces* , J. ALGEBRAIC COMB., **2023**.
- **F. Zullo:** *Multi-orbit cyclic subspace codes and linear sets*, JFINITE FIELDS AND THEIR APPLICATIONS, **2023**.
- **C. Castello, H. Gluesing-Luerssen, O.P., F. Zullo:** *Quasi-optimal cyclic orbit codes*, DESIGNS, CODES AND CRYPTOGRAPHY, **2026**.
- **C. Castello, P. Santonastaso:** *Asymptotically optimal cyclic subspace codes*, *arXiv.2507.09290*, **2025**.

Optimal cyclic orbit codes

$\mathcal{C} = Orb(V)$ optimal cyclic orbit code $\quad [n, d = 2k-2, \frac{q^n-1}{q-1}, k]_q$

Optimal cyclic orbit codes

$\mathcal{C} = Orb(V)$ optimal cyclic orbit code $\quad [n, d = 2k-2, \frac{q^n-1}{q-1}, k]_q$

Conjecture [A.-L. Trautmann, F. Manganiello, M. Braun and J. Rosenthal, IEEE TIT, **2013.]**

We conjecture that for any prime power q and positive integers k and n, we can construct optimal cyclic subspace codes $\mathcal{C} \subset \mathcal{G}_q(n,k)$, i.e. $d(\mathcal{C}) = 2k-2$ and $|\mathcal{C}| = \frac{q^n-1}{q-1}$.

Construction of optimal cyclic orbit codes

- **A.-S. Elsenhans, A. Kohnert** *Constructing network codes using Möbius transformations*, PREPRINT, **2010**, $\rightarrow$ $q = 2$, $n \geq 4k - 6$
- **E. Ben-Sasson, T. Etzion, A. Gabizon and N. Raviv:** *Subspace polynomials and cyclic subspace codes*, IEEE TRANSACTION ON INFORMATION THEORY, **2016**. $\rightarrow$ k, q and infinitely many values of n
- **K. Otal and F. Özbudak:** *Cyclic subspace codes via subspace polynomials*, DES. CODES CRYPTOGR.,**2017**. $\rightarrow$ k, q and infinitely many values of n

Construction of optimal cyclic orbit codes

- **A.-S. Elsenhans, A. Kohnert** *Constructing network codes using Möbius transformations*, PREPRINT, **2010**, $\rightarrow$ $q = 2$, $n \geq 4k - 6$
- **E. Ben-Sasson, T. Etzion, A. Gabizon and N. Raviv:** *Subspace polynomials and cyclic subspace codes*, IEEE TRANSACTION ON INFORMATION THEORY, **2016**. $\rightarrow$ k, q and infinitely many values of n
- **K. Otal and F. Özbudak:** *Cyclic subspace codes via subspace polynomials*, DES. CODES CRYPTOGR.,**2017**. $\rightarrow$ k, q and infinitely many values of n
- **R.M. Roth, N. Raviv and I. Tamo:** *Construction of Sidon spaces with applications to coding*, IEEE TRANSACTION ON INFORMATION THEORY, **2018**.

Sidon sets $\longrightarrow$ Sidon spaces

Additive Case

Sidon sets $\longrightarrow$ Sidon spaces

Additive Case

$(G, +)$ abelian group, $S \subset G$ *Sidon set*

Sidon sets $\longrightarrow$ Sidon spaces

Additive Case
$(G,+)$ abelian group, $S \subset G$ *Sidon set*

$$\text{for every } a,b,c,d \in S$$
$$a+b=c+d \quad \Longrightarrow \quad \{a,b\}=\{c,d\}.$$

Sidon sets $\longrightarrow$ Sidon spaces

Additive Case

$(G, +)$ abelian group, $S \subset G$ *Sidon set*

$$\text{for every } a, b, c, d \in S$$
$$a + b = c + d \quad \Longrightarrow \quad \{a, b\} = \{c, d\}.$$

Linear Case

$\mathbb{F}/\mathbb{K}$ field extension, $S \leq_{\mathbb{K}} \mathbb{F}$ *Sidon space*

Sidon sets $\longrightarrow$ Sidon spaces

Additive Case

$(G,+)$ abelian group, $S \subset G$ *Sidon set*

$$\text{for every } a,b,c,d \in S$$
$$a+b=c+d \quad \Longrightarrow \quad \{a,b\}=\{c,d\}.$$

Linear Case

$\mathbb{F}/\mathbb{K}$ field extension, $S \leq_{\mathbb{K}} \mathbb{F}$ *Sidon space*

$$\text{for every } a,b,c,d \in S$$
$$ab=cd \quad \Longrightarrow \quad \{a\mathbb{K},b\mathbb{K}\}=\{c\mathbb{K},d\mathbb{K}\}.$$

Sidon sets $\longrightarrow$ Sidon spaces

Additive Case

$(G,+)$ abelian group, $S \subset G$ *Sidon set*

$$\text{for every } a,b,c,d \in S$$
$$a+b=c+d \quad \Longrightarrow \quad \{a,b\}=\{c,d\}.$$

Linear Case

$\mathbb{F}/\mathbb{K}$ field extension, $S \leq_{\mathbb{K}} \mathbb{F}$ *Sidon space*

$$\text{for every } a,b,c,d \in S$$
$$ab=cd \quad \Longrightarrow \quad \{a\mathbb{K},b\mathbb{K}\}=\{c\mathbb{K},d\mathbb{K}\}.$$

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

Sidon sets $\longrightarrow$ Sidon spaces

Additive Case

$(G,+)$ abelian group, $S \subset G$ *Sidon set*

$$\text{for every } a,b,c,d \in S$$
$$a+b=c+d \implies \{a,b\}=\{c,d\}.$$

Linear Case

$\mathbb{F}/\mathbb{K}$ field extension, $S \leq_{\mathbb{K}} \mathbb{F}$ *Sidon space*

$$\text{for every } a,b,c,d \in S$$
$$ab=cd \implies \{a\mathbb{K},b\mathbb{K}\}=\{c\mathbb{K},d\mathbb{K}\}.$$

C. Bachoc, O. Serra, G. Zémor: *An analogue of Vosper's theorem for extension fields,* MATHEMATICAL PROCEEDINGS OF THE CAMBRIDGE PHILOSOPHICAL SOCIETY, **2017**.

Property [Roth, Raviv,Tamo: IEEE TIT, 2018]

$$S \in \mathcal{G}_q(n,k),\ S \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}$$

$$\mathcal{C} = Orb(S) \quad \text{optimal cyclic orbit code} \iff S \text{ Sidon space in } \mathbb{F}_{q^n}.$$

Sidon Spaces in Finite Fields

S $\mathbb{F}_q$- subspace of $\mathbb{F}_{q^n}$

Sidon Spaces in Finite Fields

S $\mathbb{F}_q$- subspace of $\mathbb{F}_{q^n}$

$S^2 =< a \cdot b \ : \ a, b \in S >_{\mathbb{F}_q}$ *square span* of S

Sidon Spaces in Finite Fields

$$S \quad \mathbb{F}_q\text{- subspace of } \mathbb{F}_{q^n}$$

$$S^2 = < a \cdot b \;:\; a, b \in S >_{\mathbb{F}_q} \quad \textit{square span} \text{ of } S$$

Theorem [Bachoc, Serra, Zémor: MATH. PROC. CAMB. PHILOS.SOC., 2017]

$S \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}$, S Sidon space, $\dim S \geq 3$

$$\dim_{\mathbb{F}_q} S^2 \geq 2 \dim S$$

Sidon Spaces in Finite Fields

$$S \quad \mathbb{F}_q\text{- subspace of } \mathbb{F}_{q^n}$$

$$S^2 = < a \cdot b \ : \ a, b \in S >_{\mathbb{F}_q} \qquad \textit{square span} \text{ of } S$$

Theorem [Bachoc, Serra, Zémor: MATH. PROC. CAMB. PHILOS.SOC., 2017]

$S \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}$, S Sidon space, $\dim S \geq 3$
$\dim_{\mathbb{F}_q} S^2 \geq 2 \dim S$

Proposition [Roth, Raviv,Tamo: IEEE TIT, 2018]

$$S \leq_{\mathbb{F}_q} \mathbb{F}_{q^n} \quad \Rightarrow \quad \dim S^2 \leq \binom{\dim S + 1}{2}.$$

Sidon Spaces in Finite Fields

$$S \quad \mathbb{F}_q\text{- subspace of } \mathbb{F}_{q^n}$$

$$S^2 =< a \cdot b \ : \ a, b \in S >_{\mathbb{F}_q} \qquad \textit{square span} \text{ of } S$$

Theorem [Bachoc, Serra, Zémor: Math. Proc. Camb. Philos.Soc., 2017]

$S \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}$, S Sidon space, $\dim S \geq 3$

$\dim_{\mathbb{F}_q} S^2 \geq 2 \dim S$

Proposition [Roth, Raviv,Tamo: IEEE TIT, 2018]

$$S \leq_{\mathbb{F}_q} \mathbb{F}_{q^n} \quad \Rightarrow \quad \dim S^2 \leq \binom{\dim S+1}{2}.$$

Sidon Spaces in Finite Fields

$$S \quad \mathbb{F}_q\text{- subspace of } \mathbb{F}_{q^n}$$

$$S^2 = < a \cdot b \ : \ a, b \in S >_{\mathbb{F}_q} \qquad \textit{square span} \text{ of } S$$

Theorem [Bachoc, Serra, Zémor: Math. Proc. Camb. Philos.Soc., 2017]

$S \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}$, S Sidon space, $\dim S \geq 3$
$\dim_{\mathbb{F}_q} S^2 \geq 2 \dim S$

Proposition [Roth, Raviv,Tamo: IEEE TIT, 2018]

$S \leq_{\mathbb{F}_q} \mathbb{F}_{q^n} \quad \Rightarrow \quad \dim S^2 \leq \binom{\dim S + 1}{2}$.
If $\dim S^2 = \binom{\dim S+1}{2}$ then S is a Sidon space.

Sidon Spaces in Finite Fields

Definition

S Sidon space in $\mathbb{F}_{q^n}$

$\dim S^2 = 2\dim S$

Sidon Spaces in Finite Fields

Definition

S Sidon space in $\mathbb{F}_{q^n}$

$\dim S^2 = 2\dim S$ *Min span Sidon space*

Sidon Spaces in Finite Fields

Definition

S Sidon space in $\mathbb{F}_{q^n}$

$\dim S^2 = 2\dim S$ *Min span Sidon space*

Definition

S Sidon space in $\mathbb{F}_{q^n}$

$\dim S^2 = \binom{\dim S+1}{2}$

Sidon Spaces in Finite Fields

Definition

S Sidon space in $\mathbb{F}_{q^n}$

$\dim S^2 = 2\dim S$ *Min span Sidon space*

Definition

S Sidon space in $\mathbb{F}_{q^n}$

$\dim S^2 = \binom{\dim S+1}{2}$ *Max span Sidon space*

Sidon Spaces in Finite Fields

Definition

S Sidon space in $\mathbb{F}_{q^n}$

$\dim S^2 = 2\dim S$ *Min span Sidon space*

Definition

S Sidon space in $\mathbb{F}_{q^n}$

$\dim S^2 = \binom{\dim S+1}{2}$ *Max span Sidon space* $\rightarrow n \geq \frac{\dim S(\dim S+1)}{2}$

Sidon Spaces in Finite Fields

Definition

S Sidon space in $\mathbb{F}_{q^n}$

$\dim S^2 = 2 \dim S$ *Min span Sidon space*

Definition

S Sidon space in $\mathbb{F}_{q^n}$

$\dim S^2 = \binom{\dim S+1}{2}$ *Max span Sidon space* $\rightarrow n \geq \frac{\dim S(\dim S+1)}{2}$

Theorem [Roth, Raviv,Tamo: IEEE TIT, 2018]

If $q > 2$ and $n \geq \frac{k(k+1)}{2}$ (or $q = 2$ and $n > \frac{k(k+1)}{2}$), then a k-dimensional max span Sidon space in $\mathbb{F}_{q^n}$ can be found in polynomial expected running time by a probabilistic algorithm.

Sidon Spaces in Finite Fields

Definition

S Sidon space in $\mathbb{F}_{q^n}$

$\dim S^2 = 2\dim S$ *Min span Sidon space*

Definition

S Sidon space in $\mathbb{F}_{q^n}$

$\dim S^2 = \binom{\dim S+1}{2}$ *Max span Sidon space* $\rightarrow$ $n \geq \frac{\dim S(\dim S+1)}{2}$

Theorem [Roth, Raviv,Tamo: IEEE TIT, 2018]

If $q > 2$ and $n \geq \frac{k(k+1)}{2}$ (or $q = 2$ and $n > \frac{k(k+1)}{2}$), then a k-dimensional max span Sidon space in $\mathbb{F}_{q^n}$ can be found in polynomial expected running time by a probabilistic algorithm.

S Sidon space in $\mathbb{F}_{q^n}$: $\dim S^2 = \Theta(\dim S)$

Sidon Spaces in Finite Fields

Definition

S Sidon space in $\mathbb{F}_{q^n}$

$\dim S^2 = 2\dim S$ *Min span Sidon space*

Definition

S Sidon space in $\mathbb{F}_{q^n}$

$\dim S^2 = \binom{\dim S+1}{2}$ *Max span Sidon space* $\rightarrow$ $n \geq \frac{\dim S(\dim S+1)}{2}$

Theorem [Roth, Raviv,Tamo: IEEE TIT, 2018]

If $q > 2$ and $n \geq \frac{k(k+1)}{2}$ (or $q = 2$ and $n > \frac{k(k+1)}{2}$), then a k-dimensional max span Sidon space in $\mathbb{F}_{q^n}$ can be found in polynomial expected running time by a probabilistic algorithm.

S Sidon space in $\mathbb{F}_{q^n}$: $\dim S^2 = \Theta(\dim S)$ *small square span*

Known constructions of Sidon Spaces with *small* square span

- ☞ $S \in \mathcal{G}_q(n,k)$, $n = kr$,

Known constructions of Sidon Spaces with *small* square span

- ☞ $S \in \mathcal{G}_q(n,k)$, $n = kr$, $\mathbb{F}_{q^k} \leq \mathbb{F}_{q^n}$,

Known constructions of Sidon Spaces with *small* square span

☞ $S \in \mathcal{G}_q(n,k)$, $n = kr$, $\mathbb{F}_{q^k} \leq \mathbb{F}_{q^n}$, $\gamma \in \mathbb{F}_{q^n} \setminus \mathbb{F}_{q^k}$.

Known constructions of Sidon Spaces with *small* square span

☞ $S \in \mathcal{G}_q(n,k)$, $n = kr$, $\mathbb{F}_{q^k} \leq \mathbb{F}_{q^n}$, $\gamma \in \mathbb{F}_{q^n} \setminus \mathbb{F}_{q^k}$.

R.M. Roth, N. Raviv and I. Tamo: *Construction of Sidon spaces with applications to coding*, IEEE Transaction on Information Theory, **2018**.

$$S = \{u + u^{q^s}\gamma \ : \ u \in \mathbb{F}_{q^k}\} \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}$$

S Sidon space in $\mathcal{G}_q(n,k)$

Known constructions of Sidon Spaces with *small* square span

☞ $S \in \mathcal{G}_q(n,k)$, $n = kr$, $\mathbb{F}_{q^k} \leq \mathbb{F}_{q^n}$, $\gamma \in \mathbb{F}_{q^n} \setminus \mathbb{F}_{q^k}$.

R.M. Roth, N. Raviv and I. Tamo: *Construction of Sidon spaces with applications to coding*, IEEE Transaction on Information Theory, **2018**.

$$S = \{u + u^{q^s}\gamma \ : \ u \in \mathbb{F}_{q^k}\} \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}$$

S Sidon space in $\mathcal{G}_q(n,k)$

$n \geq 3k$ and $\gcd(n,s) = 1$

Known constructions of Sidon Spaces with *small* square span

☞ $S \in \mathcal{G}_q(n,k)$, $n = kr$, $\mathbb{F}_{q^k} \leq \mathbb{F}_{q^n}$, $\gamma \in \mathbb{F}_{q^n} \setminus \mathbb{F}_{q^k}$.

R.M. Roth, N. Raviv and I. Tamo: *Construction of Sidon spaces with applications to coding,* IEEE TRANSACTION ON INFORMATION THEORY, **2018**.

$$S = \{u + u^{q^s}\gamma \,:\, u \in \mathbb{F}_{q^k}\} \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}$$

S Sidon space in $\mathcal{G}_q(n,k)$

$n \geq 3k$ and $\gcd(n,s) = 1$

$n = 2k$,

Known constructions of Sidon Spaces with *small* square span

☞ $S \in \mathcal{G}_q(n,k)$, $n = kr$, $\mathbb{F}_{q^k} \leq \mathbb{F}_{q^n}$, $\gamma \in \mathbb{F}_{q^n} \setminus \mathbb{F}_{q^k}$.

R.M. Roth, N. Raviv and I. Tamo: *Construction of Sidon spaces with applications to coding,* IEEE Transaction on Information Theory, **2018**.

$$S = \{u + u^{q^s}\gamma \ : \ u \in \mathbb{F}_{q^k}\} \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}$$

S Sidon space in $\mathcal{G}_q(n,k)$

$n \geq 3k$ and $\gcd(n,s) = 1$

$n = 2k, \ N_q(\gamma) \neq 1$ and $gcd(n,s) = 1$

Known constructions of Sidon Spaces with *small* square span

☞ $S \in \mathcal{G}_q(n,k),\ n = kr,\ \ \mathbb{F}_{q^k} \leq \mathbb{F}_{q^n},\ \ \gamma \in \mathbb{F}_{q^n} \setminus \mathbb{F}_{q^k}.$

R.M. Roth, N. Raviv and I. Tamo: *Construction of Sidon spaces with applications to coding,* IEEE TRANSACTION ON INFORMATION THEORY, **2018**.

$$S = \{u + u^{q^s}\gamma \ :\ u \in \mathbb{F}_{q^k}\} \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}$$

S Sidon space in $\mathcal{G}_q(n,k)$

$n \geq 3k$ and $\gcd(n,s) = 1$

$n = 2k,\ \ N_q(\gamma) \neq 1$ and $gcd(n,s) = 1$

$\dim S^2 = 2 \dim S$

Known constructions of Sidon Spaces with *small* square span

☞ $S \in \mathcal{G}_q(n,k),\ n = kr,\ \ \mathbb{F}_{q^k} \leq \mathbb{F}_{q^n},\ \ \gamma \in \mathbb{F}_{q^n} \setminus \mathbb{F}_{q^k}.$

R.M. Roth, N. Raviv and I. Tamo: *Construction of Sidon spaces with applications to coding,* IEEE TRANSACTION ON INFORMATION THEORY, **2018**.

C. Castello, O.P., P. Santonastaso. F. Zullo: *Construction and equivalence of Sidon sapces,* J. ALGEBRAIC COMB., **2023**.

$$S = \{u + u^{q^s}\gamma \ :\ u \in \mathbb{F}_{q^k}\} \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}$$

S Sidon space in $\mathcal{G}_q(n,k)$

$n \geq 3k$ and $\gcd(n,s) = 1$

$n = 2k,\ N_q(\gamma) \neq 1$ and $gcd(n,s) = 1$
$\dim S^2 = 2 \dim S$

Known constructions of Sidon Spaces with *small* square span

☞ $S \in \mathcal{G}_q(n,k)$, $n = kr$, $\mathbb{F}_{q^k} \leq \mathbb{F}_{q^n}$, $\gamma \in \mathbb{F}_{q^n} \setminus \mathbb{F}_{q^k}$.

R.M. Roth, N. Raviv and I. Tamo: *Construction of Sidon spaces with applications to coding,* IEEE Transaction on Information Theory, **2018**.

$$S = \{u + u^{q^s}\gamma \ : \ u \in \mathbb{F}_{q^k}\} \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}$$

S Sidon space in $\mathcal{G}_q(n,k)$

$n \geq 3k$ and $\mathrm{gcd}(n,s) = 1$

$n = 2k$, $N_q(\gamma) \neq 1$ and $gcd(n,s) = 1$
$\dim S^2 = 2 \dim S$

C. Castello, O.P., P. Santonastaso. F. Zullo: *Construction and equivalence of Sidon sapces,* J. Algebraic Comb., **2023**.

$$S_{f,\gamma} = \{u + f(u)\gamma \ : \ u \in \mathbb{F}_{q^k}\} \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}$$

Known constructions of Sidon Spaces with *small* square span

☞ $S \in \mathcal{G}_q(n,k)$, $n = kr$, $\mathbb{F}_{q^k} \leq \mathbb{F}_{q^n}$, $\gamma \in \mathbb{F}_{q^n} \setminus \mathbb{F}_{q^k}$.

R.M. Roth, N. Raviv and I. Tamo: *Construction of Sidon spaces with applications to coding,* IEEE Transaction on Information Theory, **2018**.

C. Castello, O.P., P. Santonastaso. F. Zullo: *Construction and equivalence of Sidon sapces,* J. Algebraic Comb., **2023**.

$$S = \{u + u^{q^s}\gamma \,:\, u \in \mathbb{F}_{q^k}\} \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}$$

S Sidon space in $\mathcal{G}_q(n,k)$

$n \geq 3k$ and $\gcd(n,s) = 1$

$n = 2k$, $N_q(\gamma) \neq 1$ and $gcd(n,s) = 1$
$\dim S^2 = 2 \dim S$

$$S_{f,\gamma} = \{u + f(u)\gamma \,:\, u \in \mathbb{F}_{q^k}\} \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}$$

$f \in \mathcal{L}_{k,q}[x] \overset{?}{\Longleftrightarrow} S_{f,\gamma}$ Sidon space in $\mathbb{F}_{q^n}$

Known constructions of Sidon Spaces with *small* square span

☞ $S \in \mathcal{G}_q(n,k)$, $n = kr$, $\mathbb{F}_{q^k} \leq \mathbb{F}_{q^n}$, $\gamma \in \mathbb{F}_{q^n} \setminus \mathbb{F}_{q^k}$.

R.M. Roth, N. Raviv and I. Tamo: *Construction of Sidon spaces with applications to coding,* IEEE TRANSACTION ON INFORMATION THEORY, **2018**.

$$S = \{u + u^{q^s}\gamma \ : \ u \in \mathbb{F}_{q^k}\} \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}$$

S Sidon space in $\mathcal{G}_q(n,k)$

$n \geq 3k$ and $\gcd(n,s) = 1$

$n = 2k$, $N_q(\gamma) \neq 1$ and $gcd(n,s) = 1$
$\dim S^2 = 2\dim S$

C. Castello, O.P., P. Santonastaso. F. Zullo: *Construction and equivalence of Sidon sapces,* J. ALGEBRAIC COMB., **2023**.

$$S_{f,\gamma} = \{u + f(u)\gamma \ : \ u \in \mathbb{F}_{q^k}\} \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}$$

$f \in \mathcal{L}_{k,q}[x] \overset{?}{\Longleftrightarrow} S_{f,\gamma}$ Sidon space in $\mathbb{F}_{q^n}$

$\dim S^2_{f,\gamma} \leq 3\dim S_{f,\gamma}$

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

$$f \in \mathcal{L}_{k,q}[x]$$

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

$$f \in \mathcal{L}_{k,q}[x] \quad u \in \mathbb{F}_{q^k}$$

$$f_u \;:\; \lambda \in \mathbb{F}_{q^k} \;:\longrightarrow f(\lambda u) - \lambda f(u) \in \mathbb{F}_{q^k}$$

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

$$f \in \mathcal{L}_{k,q}[x] \quad u \in \mathbb{F}_{q^k}$$

$$f_u \; : \; \lambda \in \mathbb{F}_{q^k} \; : \longrightarrow f(\lambda u) - \lambda f(u) \in \mathbb{F}_{q^k}$$

Definition

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

$$\ker(f_u) \cap \ker(f_v) = \mathbb{F}_q,$$

$$\forall u, v \in \mathbb{F}^*_{q^k} \text{ s.t. } u\mathbb{F}_q \neq v\mathbb{F}_q$$

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

$$f \in \mathcal{L}_{k,q}[x] \quad u \in \mathbb{F}_{q^k}$$

$$f_u \;:\; \lambda \in \mathbb{F}_{q^k} \;:\longrightarrow f(\lambda u) - \lambda f(u) \in \mathbb{F}_{q^k}$$

Definition

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

$$\ker(f_u) \cap \ker(f_v) = \mathbb{F}_q,$$

$$\forall u, v \in \mathbb{F}^*_{q^k} \text{ s.t. } u\mathbb{F}_q \neq v\mathbb{F}_q$$

Theorem

$$S_{f,\gamma} = \{u + f(u)\gamma \;:\; u \in \mathbb{F}_{q^k}\} \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}$$

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

$$f \in \mathcal{L}_{k,q}[x] \quad u \in \mathbb{F}_{q^k}$$

$$f_u \; : \; \lambda \in \mathbb{F}_{q^k} \; :\longrightarrow f(\lambda u) - \lambda f(u) \in \mathbb{F}_{q^k}$$

Definition

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

$$\ker(f_u) \cap \ker(f_v) = \mathbb{F}_q,$$

$$\forall u, v \in \mathbb{F}^*_{q^k} \text{ s.t. } u\mathbb{F}_q \neq v\mathbb{F}_q$$

Theorem

$$S_{f,\gamma} = \{u + f(u)\gamma \; : \; u \in \mathbb{F}_{q^k}\} \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}$$

$S_{f,\gamma}$ Sidon space in $\mathbb{F}_{q^n}$ $\forall n \geq 3k \iff f$ is a Sidon polynomial in $\mathbb{F}_{q^k}$

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

$$f \in \mathcal{L}_{k,q}[x] \quad u \in \mathbb{F}_{q^k}$$

$$f_u \;:\; \lambda \in \mathbb{F}_{q^k} \;:\longrightarrow f(\lambda u) - \lambda f(u) \in \mathbb{F}_{q^k}$$

Definition

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

$$\ker(f_u) \cap \ker(f_v) = \mathbb{F}_q,$$

$$\forall u, v \in \mathbb{F}^*_{q^k} \text{ s.t. } u\mathbb{F}_q \neq v\mathbb{F}_q$$

Theorem

$$S_{f,\gamma} = \{u + f(u)\gamma \;:\; u \in \mathbb{F}_{q^k}\} \leq_{\mathbb{F}_q} \mathbb{F}_{q^n}$$

$S_{f,\gamma}$ Sidon space in $\mathbb{F}_{q^n}$ $\forall n \geq 3k \iff f$ is a Sidon polynomial in $\mathbb{F}_{q^k}$

Corollary

$f \in \mathcal{L}_{k,q}[x]$ Sidon polynomial $\iff$
$\mathcal{C}_{f,\gamma} = Orb(S_{f,\gamma})$ optimal cyclic orbit code in $\mathcal{G}_q(kr, k)$ $\forall r \geq 3$

Known Sidon polynomials

	k	$f(x)$	Conditions	Year	$\mathcal{C}_{\mathbf{f},\gamma} \subseteq \mathcal{G}_q(n = rk, k)$
1)		x^{q^s}	$\gcd(s, k) = 1$	2000	$n = 2k,\ \mathrm{N}_{q^k/q}(\gamma) \neq 1$ $n \geq 3k$

Known Sidon polynomials

	k	$f(x)$	Conditions	Year	$\mathcal{C}_{\mathbf{f},\gamma} \subseteq \mathcal{G}_q(n = rk, k)$
1)		x^{q^s}	$\gcd(s, k) = 1$	2000	$n = 2k,\ \mathrm{N}_{q^k/q}(\gamma) \neq 1$ $n \geq 3k$
2)		$x^{q^s} + \delta x^{q^{s(k-1)}}$	$\gcd(s, k) = 1$ $\mathrm{N}_{q^k/q}(\delta) \neq 1$	2001/2015	$n \geq 3k$
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	$n \geq 3k$
4)	6	$x^q + \delta x^{q^4}$	$q > 4$ certain choices of δ	2018–2020	$n \geq 3k$
5)	6	$x^q + x^{q^3} + \delta x^{q^5}$	q odd $\delta^2 + \delta = 1$	2018–2020	$n \geq 3k$
6)	8	$x^q + \delta x^{q^5}$	q odd $\delta^2 = -1$	2018	$n \geq 3k$

Known Sidon polynomials

	k	$f(x)$	Conditions	Year	$\mathcal{C}_{\mathbf{f},\gamma} \subseteq \mathcal{G}_q(n = rk, k)$
1)		x^{q^s}	$\gcd(s,k) = 1$	2000	$n = 2k,\ \mathrm{N}_{q^k/q}(\gamma) \neq 1$ $n \geq 3k$
2)		$x^{q^s} + \delta x^{q^{s(k-1)}}$	$\gcd(s,k) = 1$ $\mathrm{N}_{q^k/q}(\delta) \neq 1$	2001/2015	$n \geq 3k$
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	$n \geq 3k$
4)	6	$x^q + \delta x^{q^4}$	$q > 4$ certain choices of δ	2018–2020	$n \geq 3k$
5)	6	$x^q + x^{q^3} + \delta x^{q^5}$	q odd $\delta^2 + \delta = 1$	2018–2020	$n \geq 3k$
6)	8	$x^q + \delta x^{q^5}$	q odd $\delta^2 = -1$	2018	$n \geq 3k$
7)		$x^{q^s} + \delta x^{q^{2s}}$	$\gcd(k,s) = 1$	2023	$n \geq 3k$
8)		$x^{q^s} + \delta x^{q^{s(k-1)}}$	$\gcd(s,k) = 1$ either $\mathrm{N}_{q^k/q}(\delta) \neq 1$ or k odd	2023	$n \geq 3k$

Known Sidon polynomials

	k	$f(x)$	Conditions	Year	$\mathcal{C}_{f,\gamma} \subseteq \mathcal{G}_q(n = rk, k)$
1)		x^{q^s}	$\gcd(s,k)=1$	2000	$n = 2k,\ \mathrm{N}_{q^k/q}(\gamma) \neq 1$ $n \geq 3k$
2)		$x^{q^s} + \delta x^{q^{s(k-1)}}$	$\gcd(s,k)=1$ $\mathrm{N}_{q^k/q}(\delta) \neq 1$	2001/2015	$n \geq 3k$
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	$n \geq 3k$
4)	6	$x^q + \delta x^{q^4}$	$q > 4$ certain choices of δ	2018–2020	$n \geq 3k$
5)	6	$x^q + x^{q^3} + \delta x^{q^5}$	q odd $\delta^2 + \delta = 1$	2018–2020	$n \geq 3k$
6)	8	$x^q + \delta x^{q^5}$	q odd $\delta^2 = -1$	2018	$n \geq 3k$
7)		$x^{q^s} + \delta x^{q^{2s}}$	$\gcd(k,s)=1$	2023	$n \geq 3k$
8)		$x^{q^s} + \delta x^{q^{s(k-1)}}$	$\gcd(s,k)=1$ either $\mathrm{N}_{q^k/q}(\delta) \neq 1$ or k odd	2023	$n \geq 3k$

OPEN CASE $\longrightarrow$ Existence of optimal one orbit cyclic orbit codes in $\mathcal{G}_2(2k,k)$

Known Sidon polynomials

	k	$f(x)$	Conditions	Year	$\mathcal{C}_{\mathbf{f},\gamma} \subseteq \mathcal{G}_q(n = rk, k)$
1)		x^{q^s}	$\gcd(s,k) = 1$	2000	$n = 2k,\ \mathrm{N}_{q^k/q}(\gamma) \neq 1$ $n \geq 3k$
2)		$x^{q^s} + \delta x^{q^{s(k-1)}}$	$\gcd(s,k) = 1$ $\mathrm{N}_{q^k/q}(\delta) \neq 1$	2001/2015	$n \geq 3k$
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	$n \geq 3k$
4)	6	$x^q + \delta x^{q^4}$	$q > 4$ certain choices of δ	2018–2020	$n \geq 3k$
5)	6	$x^q + x^{q^3} + \delta x^{q^5}$	q odd $\delta^2 + \delta = 1$	2018–2020	$n \geq 3k$
6)	8	$x^q + \delta x^{q^5}$	q odd $\delta^2 = -1$	2018	$n \geq 3k$
7)		$x^{q^s} + \delta x^{q^{2s}}$	$\gcd(k,s) = 1$	2023	$n \geq 3k$
8)		$x^{q^s} + \delta x^{q^{s(k-1)}}$	$\gcd(s,k) = 1$ either $\mathrm{N}_{q^k/q}(\delta) \neq 1$ or k odd	2023	$n \geq 3k$

OPEN CASE $\longrightarrow$ Existence of optimal one orbit cyclic orbit codes in $\mathcal{G}_2(2k,k)$
$k = 3, 4\ \nexists$ (by an exhaustive computational research)

Quasi-optimal orbit codes

$\mathcal{C} = Orb(V)$ quasi-optimal cyclic orbit code $\quad [n, d = 2(k-2), \frac{q^n-1}{q-1}, k]_q$

Quasi-optimal orbit codes

$\mathcal{C} = Orb(V)$ quasi-optimal cyclic orbit code $\quad [n, d = 2(k-2), \frac{q^n-1}{q-1}, k]_q$

C. Castello, H. Gluesing-Luerssen, O.P., F. Zullo: *Quasi-optimal cyclic orbit codes*, Designs, Codes and Cryptography, **2026**.

Quasi-optimal orbit codes

$\mathcal{C} = Orb(V)$ quasi-optimal cyclic orbit code $\quad [n, d = 2(k-2), \frac{q^n-1}{q-1}, k]_q$

C. Castello, H. Gluesing-Luerssen, O.P., F. Zullo: *Quasi-optimal cyclic orbit codes*, DESIGNS, CODES AND CRYPTOGRAPHY, **2026**.

Theorem

If n is even, then there exist quasi-optimal full-length orbit codes in $\mathcal{G}_q(n,k)$ for every $3 \leq k \leq \frac{n}{2}$ and for every $q \geq 2$.

Open problems and further results

- To seek efficient decoding algorithms for cyclic subspace codes more general than desarguesian spread codes.

Open problems and further results

- To seek efficient decoding algorithms for cyclic subspace codes more general than desarguesian spread codes.
- Seek constructions of multi-orbit cyclic codes that reach the anticode bound at least asymptotically.

Open problems and further results

- To seek efficient decoding algorithms for cyclic subspace codes more general than desarguesian spread codes.
- Seek constructions of multi-orbit cyclic codes that reach the anticode bound at least asymptotically.
- Existence of $\mathcal{S}_q(t, k, n)$ systems when $t \geq 2$.

Open problems and further results

- To seek efficient decoding algorithms for cyclic subspace codes more general than desarguesian spread codes.
- Seek constructions of multi-orbit cyclic codes that reach the anticode bound at least asymptotically.
- Existence of $\mathcal{S}_q(t,k,n)$ systems when $t \geq 2$.
- Find more families of Sidon polynomials. What about the exceptionality of this property for q-polynomials?

Open problems and further results

- To seek efficient decoding algorithms for cyclic subspace codes more general than desarguesian spread codes.
- Seek constructions of multi-orbit cyclic codes that reach the anticode bound at least asymptotically.
- Existence of $\mathcal{S}_q(t,k,n)$ systems when $t \geq 2$.
- Find more families of Sidon polynomials. What about the exceptionality of this property for q-polynomials?
- To study $\mathbb{F}_q$-subspaces S of $\mathbb{F}_{q^n}$ such that $\dim S^2 \leq 3\dim S - 4$.

Open problems and further results

- To seek efficient decoding algorithms for cyclic subspace codes more general than desarguesian spread codes.
- Seek constructions of multi-orbit cyclic codes that reach the anticode bound at least asymptotically.
- Existence of $\mathcal{S}_q(t,k,n)$ systems when $t \geq 2$.
- Find more families of Sidon polynomials. What about the exceptionality of this property for q-polynomials?
- To study $\mathbb{F}_q$-subspaces S of $\mathbb{F}_{q^n}$ such that $\dim S^2 \leq 3\dim S - 4$.

C. Castello, A. Couvreur, O.P., F. Zullo : *Subspaces of finite field extensions with small square-span,* ONGOING PROJECT.

Open problems and further results

- To seek efficient decoding algorithms for cyclic subspace codes more general than desarguesian spread codes.
- Seek constructions of multi-orbit cyclic codes that reach the anticode bound at least asymptotically.
- Existence of $\mathcal{S}_q(t, k, n)$ systems when $t \geq 2$.
- Find more families of Sidon polynomials. What about the exceptionality of this property for q-polynomials?
- To study $\mathbb{F}_q$-subspaces S of $\mathbb{F}_{q^n}$ such that $\dim S^2 \leq 3\dim S - 4$.

C. Castello, A. Couvreur, O.P., F. Zullo : *Subspaces of finite field extensions with small square-span,* ONGOING PROJECT.

☞ $k = 4$ and S Sidon space in $\mathbb{F}_{q^n}$ with $\dim S^2 = 8 \implies 4|n$ and S is of RTT-type;

Open problems and further results

- To seek efficient decoding algorithms for cyclic subspace codes more general than desarguesian spread codes.
- Seek constructions of multi-orbit cyclic codes that reach the anticode bound at least asymptotically.
- Existence of $\mathcal{S}_q(t,k,n)$ systems when $t \geq 2$.
- Find more families of Sidon polynomials. What about the exceptionality of this property for q-polynomials?
- To study $\mathbb{F}_q$-subspaces S of $\mathbb{F}_{q^n}$ such that $\dim S^2 \leq 3\dim S - 4$.

C. Castello, A. Couvreur, O.P., F. Zullo : *Subspaces of finite field extensions with small square-span*, ONGOING PROJECT.

- $k = 4$ and S Sidon space in $\mathbb{F}_{q^n}$ with $\dim S^2 = 8 \implies 4|n$ and S is of RTT-type;
- $k = 5$ and S Sidon space in $\mathbb{F}_{q^n}$ with $\dim S^2 \leq 11$ and $n \geq 17 \implies 2,3,5,7|n$;

Open problems and further results

- To seek efficient decoding algorithms for cyclic subspace codes more general than desarguesian spread codes.
- Seek constructions of multi-orbit cyclic codes that reach the anticode bound at least asymptotically.
- Existence of $\mathcal{S}_q(t, k, n)$ systems when $t \geq 2$.
- Find more families of Sidon polynomials. What about the exceptionality of this property for q-polynomials?
- To study $\mathbb{F}_q$-subspaces S of $\mathbb{F}_{q^n}$ such that $\dim S^2 \leq 3 \dim S - 4$.

C. Castello, A. Couvreur, O.P., F. Zullo : *Subspaces of finite field extensions with small square-span,* ONGOING PROJECT.

- $k = 4$ and S Sidon space in $\mathbb{F}_{q^n}$ with $\dim S^2 = 8 \implies 4|n$ and S is of RTT-type;
- $k = 5$ and S Sidon space in $\mathbb{F}_{q^n}$ with $\dim S^2 \leq 11$ and $n \geq 17 \implies 2, 3, 5, 7|n$;
- In $\mathbb{F}_{q^n}$ with n prime, there are not Sidon spaces of dimension $k \geq 4$ with $\dim S^2 \leq 3 \dim S - 4$ when n is sufficiently large w.r.t. k.

Thank you

Thank you for your attention!