New Maximal Additive Symmetric Rank-Metric Codes

Yue Zhou
Based on a joint work with Wei Tang

Sept. 3th, 2025

yue.zhou.ovgu@gmail.com

Outline

Introduction

Introduction

- $S(n,q)$: the set of $n \times n$ symmetric matrices over $\mathbb{F}_q$.

Introduction

- $S(n,q)$: the set of $n \times n$ symmetric matrices over $\mathbb{F}_q$.

Definition

A subset $\mathcal{C} \subseteq S(n,q)$ is called a d-code if $\mathrm{rank}(A-B) \geq d$ for any distinct $A, B \in \mathcal{C}$.

- $S(n,q)$: the set of $n \times n$ symmetric matrices over $\mathbb{F}_q$.

Definition

A subset $\mathcal{C} \subseteq S(n,q)$ is called a d-code if $\mathrm{rank}(A-B) \geq d$ for any distinct $A, B \in \mathcal{C}$.

Question: What is the largest size of d-codes in $S(n,q)$?

Introduction

- $S(n,q)$: the set of $n \times n$ symmetric matrices over $\mathbb{F}_q$.

Definition

A subset $\mathcal{C} \subseteq S(n,q)$ is called a d-code if $\mathrm{rank}(A-B) \geq d$ for any distinct $A, B \in \mathcal{C}$.

Question: What is the largest size of d-codes in $S(n,q)$?

Answer for a special case: if $n = d$, then $|\mathcal{C}| \leq q^n$.

- $S(n,q)$: the set of $n \times n$ symmetric matrices over $\mathbb{F}_q$.

Definition

A subset $\mathcal{C} \subseteq S(n,q)$ is called a d-code if $\mathrm{rank}(A-B) \geq d$ for any distinct $A, B \in \mathcal{C}$.

Question: What is the largest size of d-codes in $S(n,q)$?

Answer for a special case: if $n = d$, then $|\mathcal{C}| \leq q^n$.

Hint: Compare the first rows.

A special case: $n = d$

A classical construction: let $B_a(x, y) := \mathrm{Tr}(axy)$ where $\mathrm{Tr} : \mathbb{F}_{q^n} \to \mathbb{F}_q$. Define

$$\mathcal{C} = \{B_a(x, y) : a \in \mathbb{F}_{q^n}\}.$$

A special case: $n = d$

A classical construction: let $B_a(x, y) := \mathrm{Tr}(axy)$ where $\mathrm{Tr} : \mathbb{F}_{q^n} \to \mathbb{F}_q$. Define

$$\mathcal{C} = \{B_a(x, y) : a \in \mathbb{F}_{q^n}\}.$$

When $d = n$, $\mathcal{C} \subseteq S(n, q)$ with $|\mathcal{C}| = q^n$ is equivalent to a symplectic quasifield (division ring with ~~associative~~ multiplication and ~~right distributive~~) of order q^n.

A special case: $n = d$

A classical construction: let $B_a(x, y) := \mathrm{Tr}(axy)$ where $\mathrm{Tr} : \mathbb{F}_{q^n} \to \mathbb{F}_q$. Define

$$\mathcal{C} = \{B_a(x, y) : a \in \mathbb{F}_{q^n}\}.$$

When $d = n$, $\mathcal{C} \subseteq S(n, q)$ with $|\mathcal{C}| = q^n$ is equivalent to a symplectic quasifield (division ring with ~~associative~~ multiplication and ~~right distributive~~) of order q^n.

If $\mathcal{C}$ is further additive, then $\mathcal{C}$ is equivalent to a symplectic/commutative semifield:

$$B_a(x, y) := \mathrm{Tr}(a(x * y)), \text{ for a commutative semifield multiplication } * .$$

A special case: $n = d$

A classical construction: let $B_a(x,y) := \mathrm{Tr}(axy)$ where $\mathrm{Tr} : \mathbb{F}_{q^n} \to \mathbb{F}_q$. Define

$$\mathcal{C} = \{B_a(x,y) : a \in \mathbb{F}_{q^n}\}.$$

When $d = n$, $\mathcal{C} \subseteq S(n,q)$ with $|\mathcal{C}| = q^n$ is equivalent to a symplectic quasifield (division ring with ~~associative~~ multiplication and ~~right distributive~~) of order q^n.

If $\mathcal{C}$ is further additive, then $\mathcal{C}$ is equivalent to a symplectic/commutative semifield:

$$B_a(x,y) := \mathrm{Tr}(a(x * y)), \text{ for a commutative semifield multiplication } * .$$

A classical construction problem in finite geometry. It has been conjectured that there are "many" inequivalent commutative semifields: Dickson 1905, Knuth 1966, Ganley 1981, Cohen-Ganley 1982, Coulter-Matthews 1997/Ding-Yuan 2006, Kantor 2003, Budaghyan-Helleseth 2008, Zha- Kyureghyan-Wang 2009, Pott-Z. 2013, Göloğlu-Kolsch 2023...

General case

Theorem (Schmidt 2010, 2015, and 2020)

Let $\mathcal{C}$ be a d-code in $S(n,q)$, where $\mathcal{C}$ is required to be additive if d is even. Then

$$|\mathcal{C}| \leq \begin{cases} q^{n(n-d+2)/2}, & \text{for } n-d \text{ even,} \\ q^{(n+1)(n-d+1)/2}, & \text{for } n-d \text{ odd.} \end{cases}$$

General case

Theorem (Schmidt 2010, 2015, and 2020)

Let $\mathcal{C}$ be a d-code in $S(n,q)$, where $\mathcal{C}$ is required to be additive if d is even. Then

$$|\mathcal{C}| \leq \begin{cases} q^{n(n-d+2)/2}, & \text{for } n-d \text{ even,} \\ q^{(n+1)(n-d+1)/2}, & \text{for } n-d \text{ odd.} \end{cases}$$

Definition

An additive d-code in $S(n,q)$ meeting the upper bound above is called maximal.

- Proof: using the association schemes defined on $S(n,q)$ and $\mathscr{Q}(n,q)$.
- These bounds are sharp.

Old and New Constructions

For all parameters (Schmidt 2010, 2015):

- if $n-d$ is even, take $\gcd(s,n)=1$, a direct construction:

$$\mathcal{C} = \left\{ S(x,y) = \mathrm{Tr}(a_0 xy) + \sum_{i=1}^{(n-d)/2} \mathrm{Tr}(a_i(xy^{q^{is}} + yx^{q^{is}})) : a_i \in \mathbb{F}_{q^n} \right\};$$

- if $n-d$ is odd, given a $(d+2)$-code $\mathcal{C}$ in $S(n+1,q)$ and take an n-dim subspace

$$\mathcal{C}^* = \{S|_W : S \in \mathcal{C}\}, \qquad \text{puncturing w.r.t. } W$$

where W is an n-dim subspace of $\mathbb{F}_q^{n+1}$.

Known constructions for $d < n$

Two extra inequivalent constructions of additive 2-codes:

- For n even,

$$\mathcal{S} = \left\{ \mathrm{Tr}\left(a_0 xy + \sum_{i=1}^{m-2} a_i \left(x^{q^{st}} y + y^{q^{st}} x \right) + \epsilon b \left(x^{q^{s(m-1)}} y + y^{q^{s(m-1)}} x \right) + a x^{q^{sm}} y \right) : \quad a_0, \ldots, a_{m-2} \in \mathbb{F}_{q^{2m}}, a, b \in \mathbb{F}_{q^m} \right\},$$

where q is odd and $N_{q^{2m}/q^m}(\epsilon) \in \not\square_{q^m}$; see (Longobardi, Lunardon, Trombetti, Z. 2020).

Known constructions for $d < n$

Two extra inequivalent constructions of additive 2-codes:

- For n even,

$$\mathcal{S} = \left\{ \mathrm{Tr}\left(a_0 xy + \sum_{i=1}^{m-2} a_i \left(x^{q^{st}} y + y^{q^{st}} x \right) + \epsilon b \left(x^{q^{s(m-1)}} y + y^{q^{s(m-1)}} x \right) + a x^{q^{sm}} y \right) : \quad a_0, \ldots, a_{m-2} \in \mathbb{F}_{q^{2m}}, a, b \in \mathbb{F}_{q^m} \right\},$$

  where q is odd and $N_{q^{2m}/q^m}(\epsilon) \in \not\square_{q^m}$; see (Longobardi, Lunardon, Trombetti, Z. 2020).

- For n odd, let $\mathcal{C}$ be a maximum 2-code in $S(n-1, q)$,

$$\mathcal{C}^* = \left\{ M(A, v) : A \in \mathcal{C}, v \in \mathbb{F}_q^{n-1} \right\},$$

  where $M(A, v) = \begin{pmatrix} 0 & v \\ v^T & A \end{pmatrix}$; see (Z. 2020).

A new construction

Theorem (Tang, Z. 2025+)

Let $n = 2k$ *with* $k = 3, 4, 5$, s *such that* $\gcd(s, 2k) = 1$. *For odd prime power* q, *the following set of symmetric bilinear forms is a maximal additive* $(n-2)$*-code*

$$\left\{ \mathrm{Tr}\left(b_0 x^{q^k} y + b_1 \left(x^{q^{s(k-1)}} y + y^{q^{s(k-1)}} x \right) + \eta b_2 \left(x^{q^{s(k-2)}} y + y^{q^{s(k-2)}} x \right) \right) : b_0, b_2 \in \mathbb{F}_{q^k}, b_1 \in \mathbb{F}_{q^{2k}} \right\}.$$

where $\eta \in \not\square_{q^n}$.

A new construction

Theorem (Tang, Z. 2025+)

Let $n = 2k$ with $k = 3, 4, 5$, s such that $\gcd(s, 2k) = 1$. For odd prime power q, the following set of symmetric bilinear forms is a maximal additive $(n-2)$-code

$$\left\{ \mathrm{Tr}\left(b_0 x^{q^k} y + b_1 \left(x^{q^{s(k-1)}} y + y^{q^{s(k-1)}} x \right) + \eta b_2 \left(x^{q^{s(k-2)}} y + y^{q^{s(k-2)}} x \right) \right) : b_0, b_2 \in \mathbb{F}_{q^k}, b_1 \in \mathbb{F}_{q^{2k}} \right\}.$$

where $\eta \in \not\square_{q^n}$.

- It is symmetric because $\mathrm{Tr}(b_0 x^{q^k} y) = \mathrm{Tr}(\frac{b_0}{2} x^{q^k} y + \frac{b_0}{2} x y^{q^k})$.

A new construction

Theorem (Tang, Z. 2025+)

Let $n = 2k$ with $k = 3, 4, 5$, s such that $\gcd(s, 2k) = 1$. For odd prime power q, the following set of symmetric bilinear forms is a maximal additive $(n-2)$-code

$$\left\{ \mathrm{Tr}\left(b_0 x^{q^k} y + b_1 \left(x^{q^{s(k-1)}} y + y^{q^{s(k-1)}} x \right) + \eta b_2 \left(x^{q^{s(k-2)}} y + y^{q^{s(k-2)}} x \right) \right) : b_0, b_2 \in \mathbb{F}_{q^k}, b_1 \in \mathbb{F}_{q^{2k}} \right\}.$$

where $\eta \in \not\square_{q^n}$.

- It is symmetric because $\mathrm{Tr}(b_0 x^{q^k} y) = \mathrm{Tr}(\frac{b_0}{2} x^{q^k} y + \frac{b_0}{2} x y^{q^k})$.
- One only has to prove it for $s = 1$; see [Theorem 3.2, Neri, Santonastaso, Zullo 2022], [Gow 2009].

Proof

$|\mathcal{C}| = q^{2n} = q^{n(n-d+2)/2}$, $d = n - 2$.

Proof

$|\mathcal{C}| = q^{2n} = q^{n(n-d+2)/2}$, $d = n-2$.

$$\begin{aligned} &\mathrm{Tr}\left(b_0 x^{q^k} y + b_1\left(x^{q^{k-1}} y + y^{q^{k-1}} x\right) + \eta b_2\left(x^{q^{k-2}} y + y^{q^{k-2}} x\right)\right) \\ =&\mathrm{Tr}\left(y\left(b_0 x^{q^k} + b_1 x^{q^{k-1}} + (b_1 x)^{q^{k+1}} + \eta b_2 x^{q^{k-2}} + (\eta b_2 x)^{q^{k+2}}\right)\right) = \mathrm{Tr}(y\ g(x)). \end{aligned}$$

Goal: To show that the q-polynomial $g(x)$ has at most q^2 roots.

Proof

$|\mathcal{C}| = q^{2n} = q^{n(n-d+2)/2}$, $d = n-2$.

$$\begin{aligned} &\operatorname{Tr}\left(b_0 x^{q^k} y + b_1\left(x^{q^{k-1}} y + y^{q^{k-1}} x\right) + \eta b_2\left(x^{q^{k-2}} y + y^{q^{k-2}} x\right)\right) \\ =&\operatorname{Tr}\left(y\left(b_0 x^{q^k} + b_1 x^{q^{k-1}} + (b_1 x)^{q^{k+1}} + \eta b_2 x^{q^{k-2}} + (\eta b_2 x)^{q^{k+2}}\right)\right) = \operatorname{Tr}(y\ g(x)). \end{aligned}$$

Goal: To show that the q-polynomial $g(x)$ has at most q^2 roots. $\Leftrightarrow$ the rank of its Dickson matrix is at least $n-2$:

$$D(f) := \begin{pmatrix} a_0 & a_1 & \cdots & a_{n-1} \\ a_{n-1}^q & a_0^q & \cdots & a_{n-2}^q \\ \vdots & \vdots & \ddots & \vdots \\ a_1^{q^{n-1}} & a_2^{q^{n-1}} & \cdots & a_0^{q^{n-1}} \end{pmatrix} \in \mathbb{F}_{q^n}^{n \times n},$$

where $f := \sum_{i=0}^{n-1} a_i X^{q^i} \in \mathbb{F}_{q^n}[X]$.

The i-th row of $D(f)$ is essentially $f^{q^i} \pmod{X^{q^n} - X}$.

Proof (Continued)

$$g(x) = b_0 x^{q^k} + b_1 x^{q^{k-1}} + (b_1 x)^{q^{k+1}} + \eta b_2 x^{q^{k-2}} + (\eta b_2 x)^{q^{k+2}}$$

$g(x)$ has at most q^2 roots $\Leftrightarrow$ the rank of its Dickson matrix is at least $n-2$

$\Leftarrow \exists$ $(n-2)\times(n-2)$ *submatrices* D_i*'s of* $D(g)$ *such that* $\det(D_i) = 0$ *for all* i *cannot happen except for* $b_0 = b_1 = b_2 = 0$.

For $k = 3$, $n = 2k = 6$:

$$D(g) = \begin{pmatrix} 0 & \eta b_2 & b_1 & b_0 & b_1^{q^4} & (\eta b_2)^{q^5} \\ \eta b_2 & 0 & (\eta b_2)^q & b_1^q & b_0^q & b_1^{q^5} \\ b_1 & (\eta b_2)^q & 0 & (\eta b_2)^{q^2} & b_1^{q^2} & b_0^{q^2} \\ b_0 & b_1^q & (\eta b_2)^{q^2} & 0 & (\eta b_2)^{q^3} & b_1^{q^3} \\ b_1^{q^4} & b_0^q & b_1^{q^2} & (\eta b_2)^{q^3} & 0 & (\eta b_2)^{q^4} \\ (\eta b_2)^{q^5} & b_1^{q^5} & b_0^{q^2} & b_1^{q^3} & (\eta b_2)^{q^4} & 0 \end{pmatrix}$$

Proof (Continued, for $k = 3$, $n = 2k = 6$)

Take two 4×4 submatrices of $D(g)$:

$$D_4 = \begin{pmatrix} 0 & \eta b_2 & b_1 & b_0 \\ \eta b_2 & 0 & (\eta b_2)^q & b_1^q \\ b_1 & (\eta b_2)^q & 0 & (\eta b_2)^{q^2} \\ b_0 & b_1^q & (\eta b_2)^{q^2} & 0 \end{pmatrix}, \hat{D}_4 = \begin{pmatrix} 0 & \eta b_2 & b_0 & b_1^{q^4} \\ \eta b_2 & 0 & b_1^q & b_0^q \\ b_0 & b_1^q & 0 & (\eta b_2)^{q^3} \\ b_1^{q^4} & b_0^q & (\eta b_2)^{q^3} & 0 \end{pmatrix}.$$

$\det(D_4) = (b_0(\eta b_2)^q)^2 + (\eta b_2)^{2(q^2+1)} + b_1^{2(q+1)} - 2(b_0(\eta b_2)^{q^2+q+1} + b_0(\eta b_2)^q b_1^{q+1} + (\eta b_2)^{q^2+1} b_1^{q+1}) = 0$

implies

$$(b_0(\eta b_2)^q + (\eta b_2)^{q^2+1} - b_1^{q+1})^2 = 4 b_0 (\eta b_2)^{q^2+q+1}.$$

- As $b_0, b_2 \in \mathbb{F}_{q^k}$ and $b_1 \in \mathbb{F}_{q^{2k}}$, it contradicts to $\eta \in \not\square_{q^6}$ if $b_0, b_2 \neq 0$.
- For $b_0 = 0$ or $b_2 = 0$, we also need the determinant of $\hat{D}_4$.

Proof (Continued, for $k = 5$, $n = 2k = 10$)

$$\begin{pmatrix}
0 & 0 & 0 & \eta b_2 & b_1 & b_0 & b_1^{q^6} & (\eta b_2)^{q^7} & 0 & 0 \\
0 & 0 & 0 & 0 & (\eta b_2)^q & b_1^q & b_0^q & b_1^{q^7} & (\eta b_2)^{q^8} & 0 \\
0 & 0 & 0 & 0 & 0 & (\eta b_2)^{q^2} & b_1^{q^2} & b_0^{q^2} & b_1^{q^8} & (\eta b_2)^{q^9} \\
\eta b_2 & 0 & 0 & 0 & 0 & 0 & (\eta b_2)^{q^3} & b_1^{q^3} & b_0^{q^3} & b_1^{q^9} \\
b_1 & (\eta b_2)^q & 0 & 0 & 0 & 0 & 0 & (\eta b_2)^{q^4} & b_1^{q^4} & b_0^{q^4} \\
b_0 & b_1^q & (\eta b_2)^{q^2} & 0 & 0 & 0 & 0 & 0 & (\eta b_2)^{q^5} & b_1^{q^5} \\
b_1^{q^6} & b_0^q & b_1^{q^2} & (\eta b_2)^{q^3} & 0 & 0 & 0 & 0 & 0 & (\eta b_2)^{q^6} \\
(\eta b_2)^{q^7} & b_1^{q^7} & b_0^{q^2} & b_1^{q^3} & (\eta b_2)^{q^4} & 0 & 0 & 0 & 0 & 0 \\
0 & (\eta b_2)^{q^8} & b_1^{q^8} & b_0^{q^3} & b_1^{q^4} & (\eta b_2)^{q^5} & 0 & 0 & 0 & 0 \\
0 & 0 & (\eta b_2)^{q^9} & b_1^{q^9} & b_0^{q^4} & b_1^{q^5} & (\eta b_2)^{q^6} & 0 & 0 & 0
\end{pmatrix}$$

We need to compute the determinants of two 8×8 principal submatrices M_1 and M_2 by removing the last two (the 5th and 10th) columns/rows .

Proof (Continued, for $k = 5$, $n = 2k = 10$)

Suppose that $\det(M_1) = 0$. By a long ... computation with the help of Maple,

$$(A_1 - B_1 - C_1 + D_1 - E_1 + F_1 + G_1 - H_1 + I_1 - J_1)^2 = 4(\eta b_2)^{q^4+q^3+q^2+q+1}\Delta_1,$$

where

$$\Delta_1 = (b_1^{q^7+q^6}(\eta b_2)^{q^2} - b_0 b_1^{q^7+q^2} - b_0^{q^2} b_1^{q^6+q} + b_0^{q^2+q+1} - b_0^{q}(\eta b_2)^{q^2+q^7} + b_1^{q^2+q}(\eta b_2)^{q^7})$$

and $A_1 = b_0^{q^2+1}(\eta b_2)^{q^3+q}$, $B_1 = b_0 b_1^{q^3+q^2}(\eta b_2)^{q}$, $C_1 = b_0^{q} b_1^{q^3+1}(\eta b_2)^{q^2}$,
$D_1 = b_0^{q}(\eta b_2)^{q^4+q^2+1}$, $E_1 = b_0^{q^2} b_1^{q+1}(\eta b_2)^{q^3}$, $F_1 = b_1^{q^3+q^2+q+1}$, $G_1 = b_1^{q^7+1}(\eta b_2)^{q^2+q^3}$,
$H_1 = b_1^{q+q^2}(\eta b_2)^{q^4+1}$, $I_1 = b_1^{q^6+q^3}(\eta b_2)^{q^2+q}$, $J_1 = (\eta b_2)^{q+q^2+q^3+q^7}$.

Proof (Continued, for $k = 5$, $n = 2k = 10$)

Suppose that $\det(M_1) = 0$. By a long ... computation with the help of Maple,

$$(A_1 - B_1 - C_1 + D_1 - E_1 + F_1 + G_1 - H_1 + I_1 - J_1)^2 = 4(\eta b_2)^{q^4+q^3+q^2+q+1}\Delta_1,$$

where

$$\Delta_1 = (b_1^{q^7+q^6}(\eta b_2)^{q^2} - b_0 b_1^{q^7+q^2} - b_0^{q^2} b_1^{q^6+q} + b_0^{q^2+q+1} - b_0^q(\eta b_2)^{q^2+q^7} + b_1^{q^2+q}(\eta b_2)^{q^7})$$

and $A_1 = b_0^{q^2+1}(\eta b_2)^{q^3+q}$, $B_1 = b_0 b_1^{q^3+q^2}(\eta b_2)^q$, $C_1 = b_0^q b_1^{q^3+1}(\eta b_2)^{q^2}$,
$D_1 = b_0^q(\eta b_2)^{q^4+q^2+1}$, $E_1 = b_0^{q^2} b_1^{q+1}(\eta b_2)^{q^3}$, $F_1 = b_1^{q^3+q^2+q+1}$, $G_1 = b_1^{q^7+1}(\eta b_2)^{q^2+q^3}$,
$H_1 = b_1^{q+q^2}(\eta b_2)^{q^4+1}$, $I_1 = b_1^{q^6+q^3}(\eta b_2)^{q^2+q}$, $J_1 = (\eta b_2)^{q+q^2+q^3+q^7}$.

Clearly, $b_0, b_2 \in \mathbb{F}_{q^5} \Rightarrow \Delta_1 \in \mathbb{F}_{q^5}$.

Proof (Continued, for $k = 5$, $n = 2k = 10$)

Suppose that $\det(M_1) = 0$. By a long ... computation with the help of Maple,

$$(A_1 - B_1 - C_1 + D_1 - E_1 + F_1 + G_1 - H_1 + I_1 - J_1)^2 = 4(\eta b_2)^{q^4+q^3+q^2+q+1}\Delta_1,$$

where

$$\Delta_1 = (b_1^{q^7+q^6}(\eta b_2)^{q^2} - b_0 b_1^{q^7+q^2} - b_0^{q^2} b_1^{q^6+q} + b_0^{q^2+q+1} - b_0^q(\eta b_2)^{q^2+q^7} + b_1^{q^2+q}(\eta b_2)^{q^7})$$

and $A_1 = b_0^{q^2+1}(\eta b_2)^{q^3+q}$, $B_1 = b_0 b_1^{q^3+q^2}(\eta b_2)^q$, $C_1 = b_0^q b_1^{q^3+1}(\eta b_2)^{q^2}$,
$D_1 = b_0^q(\eta b_2)^{q^4+q^2+1}$, $E_1 = b_0^{q^2} b_1^{q+1}(\eta b_2)^{q^3}$, $F_1 = b_1^{q^3+q^2+q+1}$, $G_1 = b_1^{q^7+1}(\eta b_2)^{q^2+q^3}$,
$H_1 = b_1^{q+q^2}(\eta b_2)^{q^4+1}$, $I_1 = b_1^{q^6+q^3}(\eta b_2)^{q^2+q}$, $J_1 = (\eta b_2)^{q+q^2+q^3+q^7}$.

Clearly, $b_0, b_2 \in \mathbb{F}_{q^5} \Rightarrow \Delta_1 \in \mathbb{F}_{q^5}$.

Then the discussion is separated into two cases depending on the value of Δ_1 and b_2.

Proof (Continued, for $k = 5$, $n = 2k = 10$)

$$(A_1 - B_1 - C_1 + D_1 - E_1 + F_1 + G_1 - H_1 + I_1 - J_1)^2 = 4(\eta b_2)^{q^4+q^3+q^2+q+1}\Delta_1.$$

- If $\Delta_1, b_2 \neq 0$, then LHD $\in \mathbb{F}_{q^{10}}$ leads to contradiction.
- If $\Delta_1 = 0$ or $b_2 = 0$, then we need $\det(M_2)$, and more complicated computations...

Proof (Continued, for $k = 5$, $n = 2k = 10$)

$$(A_1 - B_1 - C_1 + D_1 - E_1 + F_1 + G_1 - H_1 + I_1 - J_1)^2 = 4(\eta b_2)^{q^4+q^3+q^2+q+1}\Delta_1.$$

- If $\Delta_1, b_2 \neq 0$, then LHD $\in \not\square_{q^{10}}$ leads to contradiction.
- If $\Delta_1 = 0$ or $b_2 = 0$, then we need $\det(M_2)$, and more complicated computations...

For $k = 4$, $n = 2k = 8$, the proof is similar and we skip it.

Equivalence Problems

Equivalence of maximal additive d-codes in $S(n, q)$

- For a nonzero $a \in \mathbb{F}_q$, $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$, $P \in \mathrm{GL}(n, q)$ and $S_0 \in S(n, \mathbb{F}_q)$, define

$$\Phi(C) = aP^T C^\sigma P + S_0, \tag{1}$$

where $C^\sigma := (c_{ij}^\sigma)$ for $C = (c_{ij})$. Then Φ preserves the rank-distance on $S(n, q)$.

Equivalence of maximal additive d-codes in $S(n, q)$

- For a nonzero $a \in \mathbb{F}_q$, $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$, $P \in \mathrm{GL}(n, q)$ and $S_0 \in S(n, \mathbb{F}_q)$, define

$$\Phi(C) = aP^T C^\sigma P + S_0, \tag{1}$$

  where $C^\sigma := (c_{ij}^\sigma)$ for $C = (c_{ij})$. Then Φ preserves the rank-distance on $S(n, q)$.
- A map $\Phi : S(n, q) \to S(n, q)$ preserves the rank-distance only if Φ is defined as in (1) except for the case with $q = 2$ and $n = 3$. (Wan, 1996)

Equivalence of maximal additive d-codes in $S(n, q)$

- For a nonzero $a \in \mathbb{F}_q$, $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$, $P \in \mathrm{GL}(n, q)$ and $S_0 \in S(n, \mathbb{F}_q)$, define

$$\Phi(C) = aP^T C^\sigma P + S_0, \tag{1}$$

  where $C^\sigma := (c_{ij}^\sigma)$ for $C = (c_{ij})$. Then Φ preserves the rank-distance on $S(n, q)$.
- A map $\Phi : S(n, q) \to S(n, q)$ preserves the rank-distance only if Φ is defined as in (1) except for the case with $q = 2$ and $n = 3$. (Wan, 1996)

Definition

For two subsets $\mathcal{C}_1, \mathcal{C}_2 \subseteq S(n, q)$, if there exists a Φ defined as in (1) such that $\Phi(\mathcal{C}_1) = \mathcal{C}_2$, then we say $\mathcal{C}_1$ and $\mathcal{C}_2$ are equivalent.

Our construction is "new"

Comparing with the parameters of known constructions, we only have to show

$$\mathcal{T}_{n,s,\eta} := \left\{ \mathrm{Tr}\left(b_0 x^{q^k} y + b_1 \left(x^{q^{s(k-1)}} y + y^{q^{s(k-1)}} x \right) + \eta b_2 \left(x^{q^{s(k-2)}} y + y^{q^{s(k-2)}} x \right) \right) : b_0, b_2 \in \mathbb{F}_{q^k}, b_1 \in \mathbb{F}_{q^{2k}} \right\}$$

is not equivalent to

$$\mathcal{C} = \left\{ \mathrm{Tr}(a_0 xy) + \mathrm{Tr}(a_1(xy^{q^t} + yx^{q^t})) : a_0, a_1 \in \mathbb{F}_{q^{2k}} \right\}, \gcd(n,t) = 1.$$

Proof. (Routine) Assume equivalence. Comparing coefficients of q-polynomials leads to contradictions.

Theorem

For any positive integer $k > 2$, let $n = 2k$. For any $\eta_1, \eta_2 \in \not\square_q$ and any integers s_1, s_2 satisfying $0 < s_1, s_2 < 2k$ and $\gcd(s_1, n) = \gcd(s_2, n) = 1$, $\mathcal{T}_{n,s_1,\eta_1}$ and $\mathcal{T}_{n,s_2,\eta_2}$ are equivalent if and only if one of the following collections of conditions is satisfied:

(a) $s_1 \equiv s_2 \pmod{n}$, *and there are* $a \in \mathbb{F}_{q^n}$, $i \in \{0, 1, \cdots, n-1\}$ *and* $r \in \{0, \ldots, m-1\}$ *such that* $\eta_2^{q^{s_1 i}} = a^{1+q^{s_1(k-2)}} \eta_1^{p^r}$;

(b) $s_1 \equiv -s_2 \pmod{n}$, *and there are* $a \in \mathbb{F}_{q^n}$, $i \in \{0, 1, \cdots, n-1\}$ *and* $r \in \{0, \ldots, m-1\}$ *such that* $\eta_2^{q^{s_1 i}} = a^{1+q^{s_1(k+2)}} \eta_1^{p^r q^{s_1(k+2)}}$.

Conclusive Remarks

Conjecture

"Theorem"

Let $n = 2k$ ~~with $k = 3, 4, 5$~~. For odd prime power q, the following set of symmetric bilinear forms is a maximal additive $n-2$ code

$$\mathcal{C}_{new} := \left\{ \mathrm{Tr}\left(b_0 x^{q^k} y + b_1 \left(x^{q^{k-1}} y + y^{q^{k-1}} x \right) + \eta b_2 \left(x^{q^{k-2}} y + y^{q^{k-2}} x \right) \right) : b_0, b_2 \in \mathbb{F}_{q^k}, b_1 \in \mathbb{F}_{q^{2k}} \right\}.$$

where $\eta \in \square\!\!\!/_{q^n}$.

- Similar situation: maximum scattered linear sets extended from $\mathrm{PG}(1, q^8)$ to $\mathrm{PG}(1, q^{2k})$.

References: Longobardi, Marino, Trombetti, Z. A Large Family of Maximum Scattered Linear Sets of $PG(1, q^n)$ and Their Associated MRD Codes. Combinatorica 43: 681-716. 2023.

Non-additive d-codes in $S(n,q)$

A bound for non-additive 2δ-codes by Schmidt 2015,

$$|\mathcal{C}| \leq \begin{cases} q^{n((n+1)/2-\delta+1)}\frac{1+q^{1-n}}{1+q}, & \text{for odd } n, \\ q^{(n+1)(n/2-\delta+1)}\frac{1+q^{2\delta-n-1}}{1+q}, & \text{for even } n. \end{cases}$$

- When $n = 2\delta = d$, the upper bound equals q^n.

Non-additive d-codes in $S(n, q)$

A bound for non-additive 2δ-codes by Schmidt 2015,

$$|\mathcal{C}| \leq \begin{cases} q^{n((n+1)/2-\delta+1)} \frac{1+q^{1-n}}{1+q}, & \text{for odd } n, \\ q^{(n+1)(n/2-\delta+1)} \frac{1+q^{2\delta-n-1}}{1+q}, & \text{for even } n. \end{cases}$$

- When $n = 2\delta = d$, the upper bound equals q^n.
- In general, the upper bound is NOT sharp: computer results by Kiermaier and his Master student Schmidt 2016.

Non-additive d-codes in $S(n, q)$

A bound for non-additive 2δ-codes by Schmidt 2015,

$$|\mathcal{C}| \leq \begin{cases} q^{n((n+1)/2-\delta+1)} \frac{1+q^{1-n}}{1+q}, & \text{for odd } n, \\ q^{(n+1)(n/2-\delta+1)} \frac{1+q^{2\delta-n-1}}{1+q}, & \text{for even } n. \end{cases}$$

- When $n = 2\delta = d$, the upper bound equals q^n.
- In general, the upper bound is NOT sharp: computer results by Kiermaier and his Master student Schmidt 2016.
- First infinite family: When $d = 2$, $n = 3$ and $q > 2$, there are examples of non-additive 2-codes beyond the additive bound.

$$q^4 + q^3 + 1 > q^4;$$

see (Cossidente, Marino, Pavese. 2022) and some better upper bounds on 2-codes in $S(3, q)$.

Thanks for your attention!

New Maximal Additive Symmetric Rank-Metric Codes

Yue Zhou
Based on a joint work with Wei Tang

Sept. 3th, 2025

yue.zhou.ovgu@gmail.com