Linear complete symmetric rank-distance codes

Nour Alnajjarine
(Joint work with Michel Lavrauw)

Faculty of Mathematics
University of Rijeka

Finite Geometries 2025, Seventh Irsee Conference

September 2, 2025

This work is supported by the Croatian Science Foundation project number HRZZ-UIP-2020-02-5713 and by the Slovenian Research and Innovation Agency project number J1-50000

Symmetric Rank-distance codes

- An $\mathbb{F}_q$*-linear symmetric rank-distance code* is a subspace $C \leq S_n(\mathbb{F}_q)$ equipped with the rank-distance metric:

$$d(A, B) = \mathrm{rank}(A - B), \quad \text{for } A, B \in C.$$

- The *minimum distance* of C is:

$$d = d(C) = \min\{d(X, Y) : X, Y \in C, \ X \neq Y\}.$$

$\mathbb{F}_q$-linear CSRD codes:

- $\mathbb{F}_q$-linear SRD codes.
- An $\mathbb{F}_q$-linear code of min. distance d is *complete* if not contained in a larger $\mathbb{F}_q$-linear code with the same d.

Bounds on additive SRD codes

- [Schmidt, 2015]:

$$\dim(C) \leq \begin{cases} \frac{n(n-d+2)}{2} & \text{if } n-d \text{ is even,} \\ \frac{(n+1)(n-d+1)}{2} & \text{if } n-d \text{ is odd.} \end{cases} \quad (1)$$

- Constructions of additive SRD codes can be found in [Schmidt, 2015, 2020].
- Bound achieved $\Rightarrow$ MSRD code (*maximum symmetric rank distance*).
- Sphere-packing bound is achieved: SRD perfect codes $\iff$ n odd and $d = 3$ [Mushrraf and Zullo, 2025].

??

To characterize $\mathbb{F}_q$-linear CSRD codes in $M_{n\times n}(\mathbb{F}_q)$ that are **not** MSRD codes.

To classify and characterize $\mathbb{F}_q$-linear CSRD codes in $M_{3\times 3}(\mathbb{F}_q)$.

GEOMETRIC INTERPRETATION

- An $\mathbb{F}_q$-linear SRD code in $M_{n\times n}(\mathbb{F}_q) \iff$ a subspace of the projective space $\mathrm{PG}(N-1,q)$; $N=\frac{n(n+1)}{2}$.
- The set of symmetric rank-one matrices in $M_{n\times n}(\mathbb{F}_q) \iff$ the set of points of the *Veronese variety* $\mathcal{V}_n(\mathbb{F}_q)$ in $\mathrm{PG}(N-1,q)$.
- $\mathcal{V}_n(\mathbb{F}_q)$ is the image of the *Veronese embedding*:

$$\nu_n : \mathrm{PG}(n,q) \to \mathrm{PG}(N-1,q)$$
$$((x_0,\ldots,x_{n-1}) \longmapsto (x_0^n, x_0^{n-1}x_1, \cdots, x_0^{n-1}x_{n-1}, \cdots, x_0^{n-2}x_1x_2, \cdots, x_{n-1}^n).$$

- $\mathcal{V}_n^{(d-1)}(\mathbb{F}_q) \iff$ the set of symmetric matrices in $M_{n\times n}(\mathbb{F}_q)$ of rank at most d.
- A k-dimensional CSRD code in $M_{n\times n}(\mathbb{F}_q)$ of minimum distance $d \iff$ a $(k-1)$-dimensional subspace of $\mathrm{PG}(N-1,q)$ that is disjoint from $\mathcal{V}_n^{(d-1)}(\mathbb{F}_q)$ (minimum rank d) and maximal for this property.

EQUIVALENCE

- C is *linear equivalent* to $C' \iff \exists\,(A,B) \in \mathrm{GL}(n,q) \times \mathrm{GL}(n,q)$ such that $C' = ACB$.
- C is linear equivalent to $C' \iff W$ is G-equivalent to W' in $\mathrm{PG}(n^2-1,q)$; $G \leqslant \mathrm{PGL}(n^2,q)$ stabilising $\mathcal{S}_{n,n}(\mathbb{F}_q)$ the image of the *Segre embedding*:

$$\sigma_{n,n} : \mathrm{PG}(n-1,q) \times \mathrm{PG}(n-1,q) \longrightarrow \mathrm{PG}(n^2-1,q)$$

$$((x_0,\ldots,x_{n-1}),(y_0,\ldots,y_{n-1})) \longmapsto (x_0y_0, x_0y_1,\ldots,x_iy_j,\ldots,x_{n-1}y_{n-1})\,.$$

.

Symmetric rank-distance codes:

- C is *symmetric equivalent* to $C' \iff \exists\, X \in \mathrm{GL}(n,q) \times \mathrm{GL}(n,q)$ such that $C' = XCX^T$.
- C is *symmetric equivalent* to $C' \iff W$ is K-equivalent to W'; $K \leqslant \mathrm{PGL}(\frac{n(n+1)}{2},q)$ stabilising $\mathcal{V}_n(\mathbb{F}_q)$.

Equivalence classes of CSRD codes: 3×3 case

$d = 2$:

- **Theorem 1:**
  There are 3 equivalence classes of $\mathbb{F}_q$-linear CSRD codes in $M_{3\times 3}(\mathbb{F}_q)$ of minimum distance 2 for q odd. Moreover, each $\mathbb{F}_q$-linear CSRD code in $M_{3\times 3}(\mathbb{F}_q)$, q odd, of minimum distance 2 is an MSRD code.
- **Theorem 2:**
  There are 6 equivalence classes of $\mathbb{F}_q$-linear CSRD codes in $M_{3\times 3}(\mathbb{F}_q)$ of minimum distance 2 for $q \geq 4$ even, 3 of which are MSRD codes.

$d = 3$:

- MSRD codes in $M_{3\times 3}(\mathbb{F}_q)$ with $d = 3$ have dimension $3 \to$ MRD codes: Equivalence classes of MRD codes in $M_{3\times 3}(\mathbb{F}_q)$ with $d = 3 \iff$ the isotopism classes of 3-dimensional semifields.
- A 3-dimensional semifield is either a field or isotopic to a twisted field [Menichetti, 1977].
- **Lemma:** An $\mathbb{F}_q$-linear CSRD code in $M_{3\times 3}(\mathbb{F}_q)$ with $d = 3$ is an MSRD code.

Approach

A k-dimensional CSRD code in $M_{3\times 3}(\mathbb{F}_q)$ of minimum distance $d \iff$ a $(k-1)$-dimensional subspace of $\mathrm{PG}(5,q)$ that is disjoint from $\mathcal{V}^{(d-1)}(\mathbb{F}_q)$ (minimum rank d) and maximal for this property.

Representation:

The solid in $\mathrm{PG}(5,q)$ spanned by the 1st four points of the standard frame is

$$\begin{bmatrix} x & y & z \\ y & t & . \\ z & . & . \end{bmatrix} := \{ \begin{bmatrix} x & y & z \\ y & t & 0 \\ z & 0 & 0 \end{bmatrix} : (x,y,z,t) \in \mathbb{F}_q^4;\ (x,y,z,t) \neq (0,0,0,0)\}.$$

$d = 2$:

To determine solids (MSRD), planes, and lines of minimum rank 2 that are disjoint from $\mathcal{V}(\mathbb{F}_q)$ and maximal for this property.

$d = 3$:

To determine planes (MSRD) and lines of minimum rank 3 that are disjoint from $\mathcal{V}^{(2)}(\mathbb{F}_q)$ and maximal for this property.

ORBITS INVARIANTS:

- The **rank distribution of** W is

$$[r_1, r_2, r_3],$$

where

$$r_i = \# \text{ of rank } i \text{ points in } W.$$

$C \iff W$:

The **rank distribution of** C is $(1, r_1(q-1), r_2(q-1), r_3(q-1))$.

- The r**-space orbit-distribution of** W is

$$OD_r(W) = [u_1, u_2, \ldots, u_m],$$

where

u_i = # of r-spaces incident with W which belong to the orbit U_i (U_1, U_2,...,U_m are the distinct K-orbits of r-spaces in $\mathrm{PG}(5, q)$).

Points and hyperplanes of $\mathrm{PG}(5,q)$

K-orbits of points; q odd / even:

- $\mathcal{P}_1$:= Rank-one points.
- $\mathcal{P}_{2,e}$:= Exterior rank-two points / $\mathcal{P}_{2,n}$:= Rank-two points in the *nucleus plane*.
- $\mathcal{P}_{2,i}$:= Interior rank-two points / $\mathcal{P}_{2,s}$:= Rank-two points outside the nucleus plane.
- $\mathcal{P}_3$:= Rank-three points.

K-orbits of Hyperplanes:

- $\mathcal{H}_1$:={ Hyperplanes $\iff$ repeated lines in $\mathrm{PG}(2,q)$}.
- $\mathcal{H}_{2,r}$:= { Hyperplanes $\iff$ pairs of real lines in $\mathrm{PG}(2,q)$}.
- $\mathcal{H}_{2,i}$:= { Hyperplanes $\iff$ pairs of conjugate imaginary lines in $\mathrm{PG}(2,q^2)$}.
- $\mathcal{H}_3$:= { Hyperplanes $\iff$ non-singular conics in $\mathrm{PG}(2,q)$}.

Solids of minimum rank 2

K-orbits of solids in $\mathrm{PG}(5,q)$

- For q odd: there are 15 K-orbits of solids corresponding to the K-orbits of lines in $\mathrm{PG}(5,q)$ ([Lavrauw and Popiel, 2020]).
  (MSRD $\iff$ solids in $\Omega_{8,2} \cup \Omega_{14,2} \cup \Omega_{15,2}$).
- For q even: there are 15 K-orbits of solids as determined in [A., Lavrauw and Popiel, 2022].

S^K	Representatives	$OD_0(S)$	$OD_4(S)$
Ω_7	$\begin{bmatrix} x & y & z \\ y & x+\gamma y & t \\ z & t & y \end{bmatrix}$	$[0, q+1, q^2+q, q^3-q]$	$[1, 0, 1, q-1]$
Ω_{13}	$\begin{bmatrix} x & y & z \\ y & \gamma x + y & t \\ z & t & \gamma x + z \end{bmatrix}$	$[0, 1, q^2+3q, q^3-2q]$	$[0, 1, 2, q-2]$
Ω_{14}	$\begin{bmatrix} x & y & \gamma x + y + \gamma t \\ y & \gamma x + y & z \\ \gamma x + y + \gamma t & z & t \end{bmatrix}$	$[0, 1, q^2+q, q^3]$	$[0, 0, 1, q]$

Table: Geometric interpretation of the 3 equivalence classes of $\mathbb{F}_q$-linear MSRD codes in $M_{3\times 3}(\mathbb{F}_q)$ for q even, where $\mathrm{Tr}(\gamma^{-1}) = 1$ in Ω_7 and $\mathrm{Tr}(\gamma) = 1$ in Ω_{13} and Ω_{14}.

PLANES OF MINIMUM RANK 2

Theorem:

- For q odd, a plane in $\mathrm{PG}(5, q)$ of minimum rank 2 is contained in a solid in $\Omega_{8,2} \cup \Omega_{14,2} \cup \Omega_{15,2}$.
- For $q \geq 4$ even, a plane in $\mathrm{PG}(5, q)$ of minimum rank 2 with at least one rank-2 point outside the nucleus plane $\pi_{\mathcal{N}}$ is contained in a solid in $\Omega_7 \cup \Omega_{13} \cup \Omega_{14}$.

Proof.

Let π be such a plane and $P \in \pi \cap \mathcal{V}^{(2)}(\mathbb{F}_q)$. The number of solids through π in $\mathrm{PG}(5, q)$ is equal to the number of points on $\mathcal{V}(\mathbb{F}_q)$, it follows that there must be at least one solid through π which does not meet $\mathcal{V}(\mathbb{F}_q)$, unless all solids of the form $\langle \pi, Q \rangle$, with $Q \in \mathcal{V}(\mathbb{F}_q)$ are distinct. To see that this is not the case, consider the conic $\mathcal{C}(P)$ and a secant line $\langle Q, Q' \rangle$ of $\mathcal{C}(P)$ through P. Then $\langle \pi, Q \rangle = \langle \pi, Q' \rangle$.

For q even, the existence of a secant line through P is guaranteed, as π contains at least one rank-2 point outside $\pi_{\mathcal{N}}$.

□

$\pi \cap \mathcal{V}^{(2)}(\mathbb{F}_q) \subseteq \pi_{\mathcal{N}}$:

- $\pi = \pi_{\mathcal{N}}$, $\pi \cap \pi_{\mathcal{N}} = \ell \in o_{12,1}$ or $\pi \cap \pi_{\mathcal{N}} = P$ (→ 3 distinct K-orbits: $\Sigma_{\mathcal{N}}$, Σ and Σ').

Theorem:

For a plane π in $\mathrm{PG}(5, q)$ with $q \geq 4$ even, we have $r_{2,n}(\pi) = h_1(\pi)$; that is, the number of hyperplanes in $\mathcal{H}_1$ containing π equals $|\pi \cap \pi_{\mathcal{N}}|$.

- **Lemma:** For $\pi \in \Sigma$, $OD_4(\pi) = [q + 1, 0, 0, q^2]$.
- **Lemma:** For $\pi \in \Sigma'$, $OD_4(\pi) = [1, 0, 0, q^2 + q]$.

Theorem:

For $q \geq 4$ even, a plane in $\mathrm{PG}(5, q)$ disjoint from $\mathcal{V}(\mathbb{F}_q)$ and intersecting $\mathcal{V}^{(2)}(\mathbb{F}_q)$ in a nonempty subspace of $\pi_{\mathcal{N}}$ is maximal with respect to that property, i.e., it is not contained in any solid of minimum rank 2.

K-orbits of Lines in $\mathrm{PG}(5, q)$

Orbits	$[r_1, r_{2,e}, r_{2,i}, r_3]$
o_5	$[2, \frac{q-1}{2}, \frac{q-1}{2}, 0]$
o_6	$[1, q, 0, 0]$
$o_{8,1}$	$[1, 1, 0, q-1]$
$o_{8,2}$	$[1, 0, 1, q-1]$
o_9	$[1, 0, 0, q]$
o_{10}	$[0, \frac{q+1}{2}, \frac{q+1}{2}, 0]$
$o_{12,1}$	$[0, q+1, 0, 0]$
$o_{13,1}$	$[0, 2, 0, q-1]$
$o_{13,2}$	$[0, 1, 1, q-1]$
$o_{14,1}$	$[0, 3, 0, q-2]$
$o_{14,2}$	$[0, 1, 2, q-2]$
$o_{15,1}$	$[0, 1, 0, q]$
$o_{15,2}$	$[0, 0, 1, q]$
$o_{16,1}$	$[0, 1, 0, q]$
o_{17}	$[0, 0, 0, q+1]$

Orbits	$[r_1, r_{2,n}, r_{2,s}, r_3]$
o_5	$[2, 0, q-1, 0]$
o_6	$[1, 1, q-1, 0]$
$o_{8,1}$	$[1, 0, 1, q-1]$
$o_{8,3}$	$[1, 1, 0, q-1]$
o_9	$[1, 0, 0, q]$
o_{10}	$[0, 0, q+1, 0]$
$o_{12,1}$	$[0, q+1, 0, 0]$
$o_{12,3}$	$[0, 1, q, 0]$
$o_{13,1}$	$[0, 1, 1, q-1]$
$o_{13,3}$	$[0, 0, 2, q-1]$
$o_{14,1}$	$[0, 0, 3, q-2]$
$o_{15,1}$	$[0, 0, 1, q]$
$o_{16,1}$	$[0, 1, 0, q]$
$o_{16,3}$	$[0, 0, 1, q]$
o_{17}	$[0, 0, 0, q+1]$

Table: K-orbits of lines in $\mathrm{PG}(5, q)$ for q odd (left) and q even (right) [Lavrauw, Popiel, 2020]

Lines of minimum rank 2:

Lemma:

A line in $\mathrm{PG}(5,q)$ of minimum rank 2 extends to a solid in $\Omega_{8,2} \cup \Omega_{14,2} \cup \Omega_{15,2}$ for q odd and $\Omega_7 \cup \Omega_{13} \cup \Omega_{14}$ for q even.

Sketch of the proof:

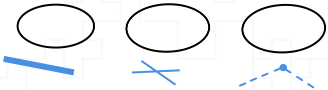
1. ℓ is contained in at least q^3 planes of minimum rank 2.
2. q odd $\longrightarrow \ell \in \Omega_{8,2} \cup \Omega_{14,2} \cup \Omega_{15,2}$.
3. q even: If $\ell \cap \mathcal{V}^2(\mathbb{F}_q) \not\subset \pi_{\mathcal{N}} \longrightarrow \ell \in \Omega_7 \cup \Omega_{13} \cup \Omega_{14}$. Else, $\ell \in o_{12,1} \cup o_{16,1}$. A solid $S \in \Omega_7$ contains a line in $o_{12,1}$ and $o_{16,1}$.

Implications on nets of conics in $\mathrm{PG}(2, q)$

- K-orbits of subspaces in $\mathrm{PG}(5, q) \iff \mathrm{PGL}(3, q)$-orbits of linear systems of conics in $\mathrm{PG}(2, q)$.
- **Open problem:** Classifying nets of conics in $\mathrm{PG}(2, q)$ with empty bases $\iff$ Classifying planes in $\mathrm{PG}(5, q)$ disjoint from $\mathcal{V}(\mathbb{F}_q)$.
- There is a unique $\mathrm{PGL}(3, q)$-orbit of nets of conics in $\mathrm{PG}(2, q)$ with conic distribution $[1, 0, 0, q^2 + q]$ for $q > 2$ even, represented by

$$\mathcal{N}_{18} = \alpha(cX_0X_2 + X_1^2) + \beta(X_0^2 + X_0X_2 + X_1X_2) + \gamma X_2^2;$$

  c is a non-admissible element of $\mathbb{F}_q$ satisfying $\mathrm{Tr}(c^{-1}) = \mathrm{Tr}(1)$
- Non-trivial perfect $\mathbb{F}_q$-linear CSRD codes in $M_{3\times 3}(\mathbb{F}_q)$ correspond to nets of conics in $\mathrm{PG}(2, q)$ that exclude singular conics.
- A net of conics with an empty base and at least one pair of lines (real or imaginary) contains a pencil of conics with an empty base:



Final Remarks

- For q odd: All $\mathbb{F}_q$-linear SRD codes in $M_{3\times 3}(\mathbb{F}_q)$ are extendable to MSRD codes.
- For q even: The only $\mathbb{F}_q$-linear SRD codes in $M_{3\times 3}(\mathbb{F}_q)$ that cannot extend to an MSRD code are the 3-dimensional CSRD codes with rank distributions $(1, 0, q^3 - 1, 0)$, $(1, 0, q^2 - 1, q^3 - q^2)$ and $(1, 0, q - 1, q^3 - q)$.
- While every MSRD code is a CSRD code, obtaining the conditions under which the converse fails remains an open question, particularly for $n > 3$.
- $\mathbb{F}_q$-linear CSRD codes in $M_{n\times n}(\mathbb{F}_q) \iff$ Linear systems of quadrics in $\mathrm{PG}(n-1, q)$.

Thank you for your attention!

REFERENCES I

- N. Alnajjarine, M. Lavrauw. “Linear complete symmetric rank-distance codes", to appear in Designs, Codes and Cryptography.
- N. Alnajjarine, M. Lavrauw, T. Popiel. Solids in the space of the Veronese surface in even characteristic. *Finite Fields and Their Applications*, **83**, (2022), 102068.
- A. Campbell, “Nets of conics in the Galois field of order 2^n”, *Bull. Amer. Math. Soc.* **34**, (1928), 481–489.
- M. Lavrauw and T. Popiel. The symmetric representation of lines in $\mathrm{PG}(\mathbb{F}_q^3 \otimes \mathbb{F}_q^3)$, *Discrete Math.* **343**, (2020), 111775.
- K. U. Schmidt. “Symmetric bilinear forms over finite fields of even characteristic", *J. Combin. Theory Ser. A*, **117**(8) (2010), 1011–1026.
- K. U. Schmidt, “Symmetric bilinear forms over finite fields with applications to coding theory", *Journal of Algebraic Combinatorics*, **42**, (2015), 635–670.