A characterization of some Linearized Reed-Solomon Codes

Valentina Astore

Joint work with M. Borello, A. Couvreur, F. Salizzoni

OpeRa 2026 - Bordeaux

Context: the geometry of codes

Coding theory

Code in $\mathbb{F}_q^n$ of dimension k

(*Up to code equivalence*)

$G = (\mathbf{g_1} \mid \mathbf{g_2} \mid \cdots \mid \mathbf{g_n})$

Reed-Solomon code

$$\begin{pmatrix} 1 & \cdots & 1 \\ a_1 & \cdots & a_n \\ \vdots & & \vdots \\ a_1^{k-1} & \cdots & a_n^{k-1} \end{pmatrix}$$

Finite geometry

Set of n projective points in $\mathbb{P}^{k-1}(\mathbb{F}_q)$

(*Up to projectivities*)

$\Pi_G = \{\mathbf{g_1}, \mathbf{g_2}, \ldots, \mathbf{g_n}\}$

Rational normal curve

$$\begin{array}{rcl} \mathbb{P}^1 & \longrightarrow & \mathbb{P}^{k-1} \\ x & \longmapsto & (1 : x : \ldots : x^{k-1}) \end{array}$$

Motivation

Hamming metric	**Sum-Rank metric**	**Rank metric**
Reed-Solomon codes	Linearized Reed-Solomon codes	Gabidulin codes
Algebraic [MZ15] and geometric [ACG13] characterizations	?	Algebraic [O07] and geometric [A+25] characterizations

[A+25] A., Borello, Calderini, and Salizzoni. "A geometric invariant of linear rank-metric codes". In: *SIAM Journal on Applied Algebra and Geometry* (2025).

[ACG13] Arbarello, Cornalba, and Griffiths. *Geometry of algebraic curves: Volume I*. (2013).

[MZ15] Mirandola and Zémor. "Critical pairs for the product Singleton bound". In: *IEEE Transactions on Information Theory* (2015).

[O07] Overbeck. "Structural attacks for public key cryptosystems based on Gabidulin codes". In: *Journal of Cryptology* (2007).

Sum-rank metric

$M = (M_1, \dots, M_t)$ vector of $\mathbb{F}_q^{m \times m}$ matrices.

The **sum-rank weight** of M is

$$w_{\mathrm{srk}}(M) = \mathrm{rk}(M_1) + \cdots + \mathrm{rk}(M_t).$$

$$M = (\underbrace{M_1}_{\in \mathbb{F}_q^{m \times m}}, \dots, M_t) \longleftrightarrow \mathbf{v} = (\underbrace{\mathbf{v_1}}_{\in \mathbb{F}_{q^m}^m} | \dots | \mathbf{v_t}).$$

$\mathbf{m = 1}$:

- $M = \mathbf{v} \in \mathbb{F}_q^t$
- $w_{\mathrm{srk}}(M) \longleftrightarrow$ Hamming weight of $\mathbf{v}$.

$\mathbf{t = 1}$:

- $M \in \mathbb{F}_q^{m \times m}$ or $\mathbf{v} \in \mathbb{F}_{q^m}^m$
- $w_{\mathrm{srk}}(M) = \mathrm{rk}(M) \longleftrightarrow$ rank weight of $\mathbf{v}$.

Sum-rank metric codes

An $[n, k, d]_{q^m/q}$ **sum-rank-metric code** $\mathcal{C}$ is a k-dimensional $\mathbb{F}_{q^m}$-linear subspace of $\mathbb{F}_{q^m}^n$.

- Length: $n = mt$.
- Dimension: k.
- Minimum distance: $d = \min\{w_{\mathsf{srk}}(\mathbf{c}) : \mathbf{c} \in \mathcal{C} \setminus \{\mathbf{0}\}\}$.

Singleton-like **bound**: $d \leq n - k + 1$.

If $d = n - k + 1 \Longrightarrow \mathcal{C}$ is called **MSRD**.

Linearized Reed-Solomon codes

Norm operator over $\mathbb{F}_{q^m}$ with respect to $\mathbb{F}_q$:

$$N_{q^m/q} : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q\,,$$
$$a \longmapsto a \cdot a^q \cdots a^{q^{m-1}} = a^{\frac{q^m-1}{q-1}}.$$

$N_i(a) = \prod_{j=0}^{i-1} a^{q^j}$ i-th truncated norm of a, for $i \geq 1$.

$(\mathbf{a}, \mathbf{b}) \in \mathbb{F}_{q^m}^t \times \mathbb{F}_{q^m}^m$ is an **evaluation pair** if

- the norms of the components of **a** are **non-zero** and **pairwise distinct**,
- the components of **b** are **linearly independent** over $\mathbb{F}_q$.

Linearized Reed-Solomon codes

Norm operator over $\mathbb{F}_{q^m}$ with respect to $\mathbb{F}_q$:

$$N_{q^m/q} : \mathbb{F}_{q^m} \longrightarrow \mathbb{F}_q\,,$$
$$a \longmapsto a \cdot a^q \cdots a^{q^{m-1}} = a^{\frac{q^m-1}{q-1}}.$$

$N_i(a) = \prod_{j=0}^{i-1} a^{q^j}$ i-th truncated norm of a, for $i \geq 1$.

$(\mathbf{a}, \mathbf{b}) \in \mathbb{F}_{q^m}^t \times \mathbb{F}_{q^m}^m$ is an **evaluation pair** if

- the norms of the components of **a** are **non-zero** and **pairwise distinct** $\Longrightarrow \mathbf{t \leq q - 1}$,
- the components of **b** are **linearly independent** over $\mathbb{F}_q$.

Linearized Reed-Solomon codes

$\big((a_1,\dots,a_t),(b_1,\dots,b_m)\big) \in \mathbb{F}_{q^m}^t \times \mathbb{F}_{q^m}^m$ evaluation pair.

A k-dimensional **Linearized Reed-Solomon code** is generated by $G = (G_1|\dots|G_t)$, with

$$G_i = \begin{pmatrix} 1 & & & \\ & N_1(a_i) & & \\ & & \ddots & \\ & & & N_{k-1}(a_i) \end{pmatrix} \underbrace{\begin{pmatrix} b_1 & \dots & b_m \\ b_1^q & \dots & b_m^q \\ \vdots & & \vdots \\ b_1^{q^{k-1}} & \dots & b_m^{q^{k-1}} \end{pmatrix}}_{k\text{-dimensional Gabidulin code over } \mathbb{F}_{q^m}^m},$$

for $i \in \{1\dots,t\}$.

Linearized Reed-Solomon codes are **MSRD** $\implies d = mt - k + 1$.

The geometry of sum-rank metric codes

Code $\mathcal{C}$ with generator matrix $G = (G_1|\dots|G_t)$.

For $i \in \{1, \dots, t\}$,

$$\mathcal{U}_i = \mathrm{colsp}_{\mathbb{F}_q}(G_i) \subseteq \mathbb{F}_{q^m}^k$$

$$\mathcal{L}_{\mathcal{U}_i} = \{\mathbf{u} : \mathbf{u} \in \mathcal{U}_i \setminus \{0\}\} \subseteq \mathbb{P}^{k-1}(\mathbb{F}_{q^m}) \quad \textbf{linear set}.$$

$\mathcal{L}_G = \mathcal{L}_{\mathcal{U}_1} \cup \dots \cup \mathcal{L}_{\mathcal{U}_t}$ is the **set of projective points associated** with $\mathcal{C}$.

[NSZ23] Neri, Santonastaso, and Zullo. "The geometry of one-weight codes in the sum-rank metric". In: *Journal of Combinatorial Theory, Series A* (2023).

q-rational normal curve

The **q-rational normal curve** X_q is defined by

$$\begin{aligned}\mathbb{P}^1 &\longrightarrow \mathbb{P}^{k-1}\\ x &\longmapsto \left(1 : x : x^{q+1} : \cdots : x^{q^{k-2}+\cdots+q+1}\right) = \left(1 : x : x^{\frac{q^2-1}{q-1}} : \cdots : x^{\frac{q^{k-1}-1}{q-1}}\right).\end{aligned}$$

The $\mathbb{F}_{q^m}$**-rational points** of X_q are

$$X_q(\mathbb{F}_{q^m}) = \{(1 : N_1(a) : N_2(a) : \cdots : N_{k-1}(a)) : a \in \mathbb{F}_{q^m}\} \cup \{P_\infty\}.$$

Reminder

$N_i(a) = \prod_{j=0}^{i-1} a^{q^j} = a^{\frac{q^i-1}{q-1}}$, for $i > 0$.

The geometry of Linearized Reed-Solomon codes

Theorem (A., Borello, Couvreur, Salizzoni. 26+)

Let $\mathcal{C}$ be a Linearized Reed-Solomon code with generator matrix G. Then

$$\mathcal{L}_G = \bigsqcup_{i=1}^{t} \mathcal{L}_{\mathcal{U}_i} \subseteq X_q(\mathbb{F}_{q^m}).$$

In particular, if $t = q - 1$,

$$\mathcal{L}_G \sqcup \{(1 : 0 : \ldots : 0), (0 : \ldots : 0 : 1)\} = X_q(\mathbb{F}_{q^m}).$$

Characterization of some Linearized Reed-Solomon codes

$\mathcal{V} \subseteq \mathbb{P}^{k-1}(\mathbb{F}_{q^m})$, $I(\mathcal{V}) = \{p \in \mathbb{F}_{q^m}[x_1, \dots, x_k] : p(\mathcal{V}) = 0\}$ vanishing ideal.

$I(\mathcal{V})_d$ homogeneous part of degree $d > 0$.

Theorem (A., Borello, Couvreur, Salizzoni. 26+)

Let $\mathcal{C}$ be an **MSRD** *code of dimension $k \leq m$ with generator matrix $G = (G_1 | \dots | G_t)$. The code $\mathcal{C}$ is a Linearized Reed-Solomon code if and only if*

- $\mathcal{C}_i = \mathrm{rowsp}_{\mathbb{F}_{q^m}}(G_i)$ *is a k-dimensional Gabidulin code over $\mathbb{F}_{q^m}^m$,*
- $\mathcal{L}_{\mathcal{U}_i} \cap \mathcal{L}_{\mathcal{U}_j} = \emptyset$,
- $I(\mathcal{L}_{\mathcal{U}_i})_{q+1} = I(\mathcal{L}_{\mathcal{U}_j})_{q+1}$,

for all $i, j \in \{1, \dots, t\}$ with $i \neq j$.

Complexity: polynomial in the defining parameters of $\mathcal{C}$.

Conclusion and Open questions

- Linearized Reed-Solomon codes $\longleftrightarrow$ q-analogue of the **rational normal curve**.
- Geometric **characterization** of Linearized Reed-Solomon codes with $k \leq m$.

What's next?

- Linearized Reed-Solomon codes with $k > m$.
- Sum-rank analogues of Reed-Muller codes.

Conclusion and Open questions

- Linearized Reed-Solomon codes $\longleftrightarrow$ q-analogue of the **rational normal curve**.
- Geometric **characterization** of Linearized Reed-Solomon codes with $k \leq m$.

What's next?

- Linearized Reed-Solomon codes with $k > m$.
- Sum-rank analogues of Reed-Muller codes.

Thank you for your attention!