A skew polynomial framework for semifields and MRD codes

Paolo Santonastaso

Polytechnic University of Bari

Finite Geometries 2025
Seventh Irsee Conference

31 August - 6 September, 2025

Rank-metric space

"Coding theory is the theory of subsets of a metric space (X, d)"

Rank-metric space

"Coding theory is the theory of subsets of a metric space (X, d)"

Rank-metric space:

- $X = M_{m \times n}(\mathbb{F}_q)$
- $d_R(A, B) = rk(A - B)$, where $A, B \in M_{m \times n}(\mathbb{F}_q)$.

Rank-metric space

"Coding theory is the theory of subsets of a metric space (X, d)"

Rank-metric space:

- $X = M_{m\times n}(\mathbb{F}_q)$
- $d_R(A, B) = rk(A - B)$, where $A, B \in M_{m\times n}(\mathbb{F}_q)$.

A rank metric code $\mathcal{C}$ is a subset of $(M_{m\times n}(\mathbb{F}_q), d_R)$.

Rank-metric space

"Coding theory is the theory of subsets of a metric space (X, d)"

Rank-metric space:

- $X = M_{m \times n}(\mathbb{F}_q)$
- $d_R(A, B) = rk(A - B)$, where $A, B \in M_{m \times n}(\mathbb{F}_q)$.

A rank metric code $\mathcal{C}$ is a subset of $(M_{m \times n}(\mathbb{F}_q), d_R)$.

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

Rank metric

Rank-metric space:

- $X = M_{m\times n}(\mathbb{F}_q)$
- $d_R(A,B) = rk(A-B)$, where $A, B \in M_{m\times n}(\mathbb{F}_q)$.

Singleton-like bound

$$|\mathcal{C}| \leq q^{\max\{m,n\}(\min\{m,n\}-d+1)}$$

Rank metric

Rank-metric space:

- $X = M_{m\times n}(\mathbb{F}_q)$
- $d_R(A,B) = rk(A-B)$, where $A, B \in M_{m\times n}(\mathbb{F}_q)$.

Singleton-like bound

$$|\mathcal{C}| \leq q^{\max\{m,n\}(\min\{m,n\}-d+1)}$$

If $|\mathcal{C}| = q^{\max\{m,n\}(\min\{m,n\}-d+1)} \Rightarrow \mathcal{C}$ **Maximum Rank Distance (MRD) code**

Rank metric

Rank-metric space:

- $X = M_{m\times n}(\mathbb{F}_q)$
- $d_R(A,B) = rk(A-B)$, where $A, B \in M_{m\times n}(\mathbb{F}_q)$.

Singleton-like bound

$$|\mathcal{C}| \leq q^{\max\{m,n\}(\min\{m,n\}-d+1)}$$

If $|\mathcal{C}| = q^{\max\{m,n\}(\min\{m,n\}-d+1)} \Rightarrow \mathcal{C}$ **Maximum Rank Distance (MRD) code**

Equivalence

$\mathcal{C}, \mathcal{C}' \subseteq M_{m\times n}(\mathbb{F}_q)$

$$\mathcal{C} \sim \mathcal{C}' \Longleftrightarrow \mathcal{C}' = A \cdot \mathcal{C}^\tau \cdot B = \{AC^\tau B : C \in \mathcal{C}\},$$

$$A \in \mathrm{GL}(m,q), B \in \mathrm{GL}(n,q), \tau \in Aut(\mathbb{F}_q)$$

Skew polynomial rings

$$n = m$$

Skew polynomial rings

$n = m$

- $\mathbb{F}_{q^n}/\mathbb{F}_q$ finite field extension

Skew polynomial rings

$n = m$

- $\mathbb{F}_{q^n}/\mathbb{F}_q$ finite field extension
- $Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) = \langle \sigma \rangle$

Skew polynomial rings

$n = m$

- $\mathbb{F}_{q^n}/\mathbb{F}_q$ finite field extension
- $Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) = \langle \sigma \rangle$

$$R = \left\{ \sum_{i=0}^{t} \alpha_i x^i : \alpha_i \in \mathbb{F}_{q^m} \right\}$$

- $$\sum_i \alpha_i x^i + \sum_i \beta_i x^i = \sum_i (\alpha_i + \beta_i) x^i$$
- $$x \cdot \alpha = \sigma(\alpha) \cdot x$$

Skew polynomial rings

$n = m$

- $\mathbb{F}_{q^n}/\mathbb{F}_q$ finite field extension
- $Gal(\mathbb{F}_{q^n}/\mathbb{F}_q) = \langle \sigma \rangle$

$$R = \left\{ \sum_{i=0}^{t} \alpha_i x^i : \alpha_i \in \mathbb{F}_{q^m} \right\}$$

- $$\sum_i \alpha_i x^i + \sum_i \beta_i x^i = \sum_i (\alpha_i + \beta_i) x^i$$

- $$x \cdot \alpha = \sigma(\alpha) \cdot x$$

$(R, +, \cdot)$

Skew polynomial ring

O. Ore: Theory of non-commutative polynomials, *Annals of Mathematics*, (1933)

Skew polynomial rings

$$R = \left\{ \sum_{i=0}^{t} \alpha_i x^i : \alpha_i \in \mathbb{F}_{q^n} \right\}$$

$$f = \sum_i \alpha_i x^i$$

$$\phi_f : \beta \in \mathbb{F}_{q^n} \longmapsto \sum_i \alpha_i \sigma^i(\beta) \in \mathbb{F}_{q^n}$$

$\mathbb{F}_q$-linear map

Skew polynomial rings

$$R = \left\{ \sum_{i=0}^{t} \alpha_i x^i : \alpha_i \in \mathbb{F}_{q^n} \right\}$$

$$f = \sum_i \alpha_i x^i$$

$$\phi_f : \beta \in \mathbb{F}_{q^n} \longmapsto \sum_i \alpha_i \sigma^i(\beta) \in \mathbb{F}_{q^n}$$

$\mathbb{F}_q$-linear map

$$\frac{R}{R(x^n - 1)} \cong \mathrm{End}_{\mathbb{F}_q}(\mathbb{F}_{q^n}) \cong M_n(\mathbb{F}_q)$$

$$rk(f) = dim_{\mathbb{F}_q}(Im(\phi_f))$$

Skew polynomial rings

Rank-metric space:

- $X = \frac{R}{R(x^n-1)} = \left\{ f = \sum_{i=0}^{n-1} \alpha_i x^i : \alpha_i \in \mathbb{F}_{q^n} \right\}$
- $rk(f) = dim_{\mathbb{F}_q}(Im(\phi_f))$
- $d_R(f,g) = rk(f-g)$

$$(M_n(\mathbb{F}_q), d_R) \cong \left(\frac{R}{R(x^n-1)}, d_R \right)$$

MRD codes

$$(M_n(\mathbb{F}_q), d_R) \cong \left(\frac{R}{R(x^n-1)}, d_R\right) \text{ rank-metric space}$$

(Generalized) Gabidulin codes	$\left\{\alpha_0 + \alpha_1 x + \ldots + \alpha_{k-1} x^{k-1} \colon \alpha_i \in \mathbb{F}_{q^n}\right\}$
(Generalized) Twisted Gabidulin codes	$\left\{\alpha_0 + \sum_{i=1}^{k-1} \alpha_i x^i + \rho(\alpha_0)\eta x^k \colon \alpha_i \in \mathbb{F}_{q^n}\right\}$
Codes from scattered polynomials	$\{\alpha_0 + \alpha_1 f(x) \colon \alpha_0, \alpha_1 \in \mathbb{F}_{q^n}\}$
Trombetti-Zhou codes	$\left\{\alpha_0' + \sum_{i=1}^{k-1} \alpha_i x^i + \gamma \alpha_k' x^k \colon \alpha_i \in \mathbb{F}_{q^n}, \alpha_0', \alpha_k' \in \mathbb{F}_{q^{n/2}}\right\}$

MRD codes

(Generalized) Gabidulin codes	$\{\alpha_0 + \alpha_1 x + \ldots + \alpha_{k-1}x^{k-1} \colon \alpha_i \in \mathbb{F}_{q^n}\}$
(Generalized) Twisted Gabidulin codes	$\left\{\alpha_0 + \sum_{i=1}^{k-1} \alpha_i x^i + \rho(\alpha_0)\eta x^k \colon \alpha_i \in \mathbb{F}_{q^n}\right\}$
Codes from scattered polynomials	$\{\alpha_0 + \alpha_1 f(x) \colon \alpha_0, \alpha_1 \in \mathbb{F}_{q^n}\}$
Trombetti-Zhou codes	$\left\{\alpha_0' + \sum_{i=1}^{k-1} \alpha_i x^i + \gamma \alpha_k' x^k \colon \alpha_i \in \mathbb{F}_{q^n}, \alpha_0', \alpha_k' \in \mathbb{F}_{q^{n/2}}\right\}$

MRD conditions

- $1 \leq k < n$

P. Delsarte: Bilinear forms over a finite field, with applications to coding theory, *Journal of Combinatorial Theory, Series A* (1978)

E. Gabidulin: Theory of codes with maximum rank distance, *Problems of information transmission*, (1985)

A. Kshevetskiy and E. Gabidulin: The new construction of rank codes, *International Symposium on Information Theory*, (2005)

MRD codes

(Generalized) Gabidulin codes	$\{\alpha_0 + \alpha_1 x + \ldots + \alpha_{k-1} x^{k-1} \colon \alpha_i \in \mathbb{F}_{q^n}\}$
(Generalized) Twisted Gabidulin codes	$\left\{\alpha_0 + \sum_{i=1}^{k-1} \alpha_i x^i + \rho(\alpha_0)\eta x^k \colon \alpha_i \in \mathbb{F}_{q^n}\right\}$
Codes from scattered polynomials	$\{\alpha_0 + \alpha_1 f(x) \colon \alpha_0, \alpha_1 \in \mathbb{F}_{q^n}\}$
Trombetti-Zhou codes	$\left\{\alpha_0' + \sum_{i=1}^{k-1} \alpha_i x^i + \gamma \alpha_k' x^k \colon \alpha_i \in \mathbb{F}_{q^n}, \alpha_0', \alpha_k' \in \mathbb{F}_{q^{n/2}}\right\}$

MRD conditions

- $1 \leq k < n$
- $\mathrm{N}_{q^n/q}(\eta) \neq (-1)^{nk}$

J. Sheekey: A new family of linear maximum rank distance codes, *Advances in Mathematics of Communications*, (2016)

G. Lunardon, R. Trombetti, and Y. Zhou: Generalized twisted Gabidulin codes, *Journal of Combinatorial Theory, Series A*, (2018)

K. Otal and F. Ozbudak: Additive rank metric codes, *IEEE Transactions on Information Theory*, (2016)

MRD codes

(Generalized) Gabidulin codes	$\left\{\alpha_0 + \alpha_1 x + \ldots + \alpha_{k-1} x^{k-1} \colon \alpha_i \in \mathbb{F}_{q^n}\right\}$
(Generalized) Twisted Gabidulin codes	$\left\{\alpha_0 + \sum_{i=1}^{k-1} \alpha_i x^i + \rho(\alpha_0)\eta x^k \colon \alpha_i \in \mathbb{F}_{q^n}\right\}$
Codes from scattered polynomials	$\{\alpha_0 + \alpha_1 f(x) \colon \alpha_0, \alpha_1 \in \mathbb{F}_{q^n}\}$
Trombetti-Zhou codes	$\left\{\alpha_0' + \sum_{i=1}^{k-1} \alpha_i x^i + \gamma \alpha_k' x^k \colon \alpha_i \in \mathbb{F}_{q^n}, \alpha_0', \alpha_k' \in \mathbb{F}_{q^{n/2}}\right\}$

D. Bartoli, B. Csajbók, A. Giannoni, G. G. Grimaldi, G. Longobardi, G. Lunardon, G. Marino, M. Montanucci, A. Neri, O. Polverino, PS, V. Smaldore, M. Timpanella, R. Trombetti, C. Zanella, Y. Zhou, F. Zullo...

MRD codes

(Generalized) Gabidulin codes	$\{\alpha_0 + \alpha_1 x + \ldots + \alpha_{k-1} x^{k-1} \colon \alpha_i \in \mathbb{F}_{q^n}\}$
(Generalized) Twisted Gabidulin codes	$\left\{\alpha_0 + \sum_{i=1}^{k-1} \alpha_i x^i + \rho(\alpha_0)\eta x^k \colon \alpha_i \in \mathbb{F}_{q^n}\right\}$
Codes from scattered polynomials	$\{\alpha_0 + \alpha_1 f(x) \colon \alpha_0, \alpha_1 \in \mathbb{F}_{q^n}\}$
Trombetti-Zhou codes	$\left\{\alpha_0' + \sum_{i=1}^{k-1} \alpha_i x^i + \gamma \alpha_k' x^k \colon \alpha_i \in \mathbb{F}_{q^n}, \alpha_0', \alpha_k' \in \mathbb{F}_{q^{n/2}}\right\}$

MRD conditions

- $1 \leq k < n$
- $\mathrm{N}_{q^n/q}(\gamma) \notin \mathbb{F}_q^{(2)}$ (q odd)

R. Trombetti and Y. Zhou: A new family of MRD codes in $\mathbb{F}_q^{2n\times 2n}$ with right and middle nuclei $\mathbb{F}_{q^n}$, *IEEE Transactions on Information Theory*, (2018)

Division Algebras

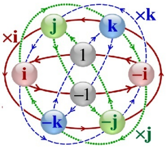
Definition

- $\mathbb{F}$ field
- $\mathbb{A}$ vector space over $\mathbb{F}$
-
$$\star : \mathbb{A} \times \mathbb{A} \to \mathbb{A}, \quad (a, b) \mapsto a \star b$$
$$(\mathbb{F}\text{-bilinear map})$$
- $a \in \mathbb{A}$,
$$L_a : b \in \mathbb{A} \longmapsto a \star b \in \mathbb{A} \quad \text{invertible}$$
$$\Downarrow$$
$$(\mathbb{A}, +, \star) \text{ division algebra}$$

- $1 \in \mathbb{A} \Rightarrow \mathbb{A}$ unital division algebra
- $\star$ associative $\Rightarrow \mathbb{A}$ associative division algebra
- $\star$ commutative $\Rightarrow \mathbb{A}$ commutative division algebra

Division algebras

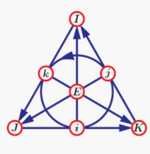
- Every field is a division algebra
- Hamilton's quaternion algebra (1843)



↓ × →	**1**	**i**	**j**	**k**
1	1	i	j	k
i	i	−1	k	−j
j	j	−k	−1	i
k	k	j	−i	−1

(non-commutative, associative division algebra)

- Graves's Octonion algebra (1843)



×	*i*	*j*	*k*	*E*	*I*	*J*	*K*
i	−1	*k*	−*j*	*I*	−*E*	−*K*	*J*
j	−*k*	−1	*i*	*J*	*K*	−*E*	−*I*
k	*j*	−*i*	−1	*K*	−*J*	*I*	−*E*
E	−*I*	−*J*	−*K*	−1	*i*	*j*	*k*
I	*E*	−*K*	*J*	−*i*	−1	−*k*	*j*
J	*K*	*E*	−*I*	−*j*	*k*	−1	−*i*
K	−*J*	*I*	*E*	−*k*	−*j*	*i*	−1

(non-commutative, non-associative division algebra)

Division algebras

$$|\mathbb{A}| \text{ finite } \Rightarrow \mathbb{A} \text{ (pre-)semifield}$$

Wedderburn's little theorem

Every associative semifield is a field

L. E. Dickson: On commutative linear algebras in which division is always uniquely possible, *Transactions of the American Mathematical Society (1906)*

- Dickson
- Hughes-Kleinfeld
- Knuth
- Cohen-Ganley
- Coulter-Matthews
- Jha-Johnson
- Dempwolff
- Kantor
- Budaghyan-Helleseth
- various subsets of [Ebert-Johnson-Marino-Polverino-Trombetti-Lunardon-Lavrauw]
- Zha-Kyureghyan-Wang
- Bierbrauer
- Pott-Zhou
- Bartoli-Bierbrauer-Kyureghyan-Giulietti-Marcugini-Pambianco
- Sheekey
- Gologlu-Kölsch, Kölsch
- Lobillo-PS-Sheekey
- ...

Why Semifields?

- projective planes;
- spreads;
- PN functions;
- relative difference sets;
- additive Hamming-metric codes;
- MRD codes with $d = n$.

Division Algebras

- $(\mathbb{A}, +, \star)$ semifield over $\mathbb{F}_q$

Division Algebras

- $(\mathbb{A}, +, \star)$ semifield over $\mathbb{F}_q$
- $a \in \mathbb{A}$,

$$L_a : b \in \mathbb{A} \longmapsto a \star b \in \mathbb{A},$$

$$L_a \in \mathrm{End}_{\mathbb{F}_q}(\mathbb{A})$$

- $$\mathcal{C}(\mathbb{A}) := \{L_a : a \in \mathbb{A}\} \subset \mathrm{End}_{\mathbb{F}_q}(\mathbb{A}) \cong M_n(\mathbb{F}_q), \quad \dim_{\mathbb{F}_q}(\mathbb{A}) = n$$

(spread set of $\mathbb{A}$)

Division Algebras

- $(\mathbb{A}, +, \star)$ semifield over $\mathbb{F}_q$
- $a \in \mathbb{A}$,

$$L_a : b \in \mathbb{A} \longmapsto a \star b \in \mathbb{A},$$

$$L_a \in \mathrm{End}_{\mathbb{F}_q}(\mathbb{A})$$

- $$\mathcal{C}(\mathbb{A}) := \{L_a : a \in \mathbb{A}\} \subset \mathrm{End}_{\mathbb{F}_q}(\mathbb{A}) \cong M_n(\mathbb{F}_q), \quad \dim_{\mathbb{F}_q}(\mathbb{A}) = n$$

(spread set of $\mathbb{A}$)

Theorem (J. De la Cruz, M. Kiermaier, A. Wassermann, and W. Willems (2016) - A. Gruica, A. Ravagnani, J. Sheekey, and F. Zullo (2023))

- $\mathcal{C}(\mathbb{A}) \subseteq M_n(\mathbb{F}_q)$ is an MRD code with $n = d$
- There is a one-to-one correspondence between *isotopy* classes of semifields and equivalence classes of MRD codes in $M_n(\mathbb{F}_q)$ with minimum distance $d = n$

MRD codes

J. Sheekey: New semifields and new MRD codes from skew polynomial rings, *Journal of the London Mathematical Society*, (2020)

J. Sheekey: New semifields and new MRD codes from skew polynomial rings, *Journal of the London Mathematical Society*, (2020)

$$(M_n(\mathbb{F}_q), d_R) \cong \left(\frac{R}{R(x^n-1)}, d_R\right)$$

MRD codes

J. Sheekey: New semifields and new MRD codes from skew polynomial rings, *Journal of the London Mathematical Society*, (2020)

$$(M_n(\mathbb{F}_q), d_R) \cong \left(\frac{R}{R(x^n-1)}, d_R \right)$$

$x^n - 1$ central element of R

Centre of skew polynomial rings

$$R = \left\{ \sum_{i=0}^{t} \alpha_i x^i : \alpha_i \in \mathbb{F}_{q^m} \right\}$$

$$Z(R) = \{F(x^n) : F(y) \in \mathbb{F}_q[y]\} \cong \mathbb{F}_q[y]$$

Codes from skew polynomial rings

Centre of skew polynomial rings

$$R = \left\{ \sum_{i=0}^{t} \alpha_i x^i : \alpha_i \in \mathbb{F}_{q^m} \right\}$$

$$Z(R) = \{F(x^n) : F(y) \in \mathbb{F}_q[y]\} \cong \mathbb{F}_q[y]$$

$y \neq F(y)$ irreducible $\Longrightarrow RF(x^n)$ two-sided maximal ideal

Codes from skew polynomial rings

Centre of skew polynomial rings

$$R = \left\{ \sum_{i=0}^{t} \alpha_i x^i : \alpha_i \in \mathbb{F}_{q^m} \right\}$$

$$Z(R) = \{ F(x^n) \colon F(y) \in \mathbb{F}_q[y] \} \cong \mathbb{F}_q[y]$$

$y \neq F(y)$ irreducible $\Longrightarrow RF(x^n)$ two-sided maximal ideal

$F(y) \in \mathbb{F}_q[y]$ irreducible polynomial, $\deg(F) = s$

Codes from skew polynomial rings

Centre of skew polynomial rings

$$R = \left\{ \sum_{i=0}^{t} \alpha_i x^i : \alpha_i \in \mathbb{F}_{q^m} \right\}$$

$$Z(R) = \{F(x^n) : F(y) \in \mathbb{F}_q[y]\} \cong \mathbb{F}_q[y]$$

$$y \neq F(y) \text{ irreducible } \Longrightarrow RF(x^n) \text{ two-sided maximal ideal}$$

$$F(y) \in \mathbb{F}_q[y] \text{ irreducible polynomial, } \deg(F) = s$$

$$\Downarrow$$

$$R_F := \frac{R}{RF(x^n)} \text{ simple and left Artinian ring}$$

Codes from skew polynomial rings

Centre of skew polynomial rings

$$R = \left\{ \sum_{i=0}^{t} \alpha_i x^i : \alpha_i \in \mathbb{F}_{q^m} \right\}$$

$$Z(R) = \{F(x^n) \colon F(y) \in \mathbb{F}_q[y]\} \cong \mathbb{F}_q[y]$$

$$y \neq F(y) \text{ irreducible } \Longrightarrow RF(x^n) \text{ two-sided maximal ideal}$$

$$F(y) \in \mathbb{F}_q[y] \text{ irreducible polynomial, } \deg(F) = s$$

$$\Downarrow$$

$$R_F := \frac{R}{RF(x^n)} \text{ simple and left Artinian ring}$$

$$\Downarrow$$

$$\varphi_F : R_F \cong M_n(\mathbb{F}_{q^s}) \text{ (by Artin-Wedderburn Theorem)}$$

Centre of skew polynomial rings

$$R = \left\{ \sum^{t} \alpha_i x^i : \alpha_i \in \mathbb{F}_{q^m} \right\}$$

$$\varphi_F : R_F = \frac{R}{RF(x^n)} \cong M_n(\mathbb{F}_{q^s})$$

$$\Downarrow$$

$$a \in R_F, \quad rk(a) := rk(\varphi_F(a))$$

$$\Downarrow$$

$$(R_F, d_R) \cong (M_n(\mathbb{F}_{q^s}), d_R)$$

$RF(x^n)$

$$\Downarrow$$

$\varphi_F : R_F \cong M_n(\mathbb{F}_{q^s})$ (by Artin-Wedderburn Theorem)

Codes from skew polynomial rings

Centre of skew polynomial rings

$$R = \left\{ \sum^{t} \alpha_i x^i : \alpha_i \in \mathbb{F}_{q^m} \right\}$$

$$\varphi_F : R_F = \frac{R}{RF(x^n)} \cong M_n(\mathbb{F}_{q^s})$$

$$\Downarrow$$

$$a \in R_F, \quad rk(a) := rk(\varphi_F(a))$$

$$\Downarrow$$

$$(R_F, d_R) \cong (M_n(\mathbb{F}_{q^s}), d_R)$$

$RF(x^n)$

$$F(y) = y - 1$$

$$R_F \cong \frac{R}{R(x^n - 1)} \cong M_n(\mathbb{F}_q)$$

MRD codes from skew polynomial rings

$$(R_F, d_R) \cong (M_n(\mathbb{F}_{q^s}), d_R)$$

Theorem (J. Sheekey, 2020)

- $\rho \in \mathrm{Aut}(\mathbb{F}_{q^n})$
- $1 \leq k < n$
- $\eta \in \mathbb{F}_{q^n}$: $\mathrm{N}_{q^n/q'}(\eta)\mathrm{N}_{q/q'}((-1)^{sk(n-1)}F(0)^k) \neq 1$

$$S(F) := \left\{\alpha_0 + \sum_{i=1}^{sk-1} \alpha_i x^i + \eta\rho(\alpha_0)x^{sk} : \alpha_i \in \mathbb{F}_{q^n}\right\} \subseteq R_F \cong M_n(\mathbb{F}_{q^s}).$$

$$\Downarrow$$

$S(F)$ is an MRD code in $M_n(\mathbb{F}_{q^s})$ with $|S(F)| = q^{nsk}$ and $d(S(F)) = n - k + 1$

MRD codes from skew polynomial rings

$$(R_F, d_R) \cong (M_n(\mathbb{F}_{q^s}), d_R)$$

Theorem (J. Sheekey, 2020)

$$S(F) := \left\{ \alpha_0 + \sum_{i=1}^{sk-1} \alpha_i x^i + \eta\rho(\alpha_0) x^{sk} : \alpha_i \in \mathbb{F}_{q^n} \right\} \subseteq R_F \cong M_n(\mathbb{F}_{q^s}).$$

MRD codes from skew polynomial rings

$$(R_F, d_R) \cong (M_n(\mathbb{F}_{q^s}), d_R)$$

Theorem (J. Sheekey, 2020)

$$S(F) := \left\{ \alpha_0 + \sum_{i=1}^{sk-1} \alpha_i x^i + \eta\rho(\alpha_0) x^{sk} : \alpha_i \in \mathbb{F}_{q^n} \right\} \subseteq R_F \cong M_n(\mathbb{F}_{q^s}).$$

$s = 1$, $F(y) = y - 1$ and $\eta = 0$

$$S(F) = \left\{ \alpha_0 + \sum_{i=1}^{k-1} \alpha_i x^i : \alpha_i \in \mathbb{F}_{q^n} \right\} \subseteq R_F = \frac{R}{R(x^n - 1)} \cong M_n(\mathbb{F}_q)$$

(Generalized) Gabidulin codes

MRD codes from skew polynomial rings

$$(R_F, d_R) \cong (M_n(\mathbb{F}_{q^s}), d_R)$$

Theorem (J. Sheekey, 2020)

$$S(F) := \left\{ \alpha_0 + \sum_{i=1}^{sk-1} \alpha_i x^i + \eta\rho(\alpha_0) x^{sk} : \alpha_i \in \mathbb{F}_{q^n} \right\} \subseteq R_F \cong M_n(\mathbb{F}_{q^s}).$$

$s = 1$, $F(y) = y - 1$ and $\eta \neq 0$

$$S(F) = \left\{ \alpha_0 + \sum_{i=1}^{k-1} \alpha_i x^i + \eta\rho(\alpha_0) : \alpha_i \in \mathbb{F}_{q^n} \right\} \subseteq R_F = \frac{R}{R(x^n - 1)} \cong M_n(\mathbb{F}_q)$$

(Generalized) Twisted Gabidulin codes

MRD codes from skew polynomial rings

$$(R_F, d_R) \cong (M_n(\mathbb{F}_{q^s}), d_R)$$

Theorem (J. Sheekey, 2020)

$$S(F) := \left\{ \alpha_0 + \sum_{i=1}^{sk-1} \alpha_i x^i + \eta\rho(\alpha_0) x^{sk} : \alpha_i \in \mathbb{F}_{q^n} \right\} \subseteq R_F \cong M_n(\mathbb{F}_{q^s}).$$

$k = 1$ and $\eta = 0$

$$S(F) = \left\{ \alpha_0 + \sum_{i=1}^{s-1} \alpha_i x^i : \alpha_i \in \mathbb{F}_{q^n} \right\} \subseteq R_F = \frac{R}{R(F(x^n))} \cong M_n(\mathbb{F}_{q^s})$$

Sandler's semifields/cyclic semifields

MRD codes from skew polynomial rings

$$(R_F, d_R) \cong (M_n(\mathbb{F}_{q^s}), d_R)$$

Theorem (J. Sheekey, 2020)

- $\rho \in \mathrm{Aut}(\mathbb{F}_{q^n})$
- $1 \leq k < n$
- $\mathrm{N}_{q^n/q'}(\eta)\mathrm{N}_{q/q'}((-1)^{sk(n-1)}F(0)^k) \neq 1$

$$S(F) := \left\{ \alpha_0 + \sum_{i=1}^{sk-1} \alpha_i x^i + \eta\rho(\alpha_0)x^{sk} : \alpha_i \in \mathbb{F}_{q^n} \right\} \subseteq R_F \cong M_n(\mathbb{F}_{q^s}).$$

$$\Downarrow$$

$S(F)$ is an MRD code in $M_n(\mathbb{F}_{q^s})$

Theorem (J. Sheekey, 2020)

The family $S(F)$ contains new semifields and new MRD codes for infinite choices of s and n (and k).

Codes from skew polynomial rings

$$(R_F, d_R) \cong (M_n(\mathbb{F}_{q^s}), d_R)$$

F.J. Lobillo, PS, and J. Sheekey: Quotients of skew polynomial rings: new constructions of division algebras and MRD codes, *arXiv preprint arXiv:2502.13531,* (2025)

Codes from skew polynomial rings

$$(R_F, d_R) \cong (M_n(\mathbb{F}_{q^s}), d_R)$$

- n even
- q odd

Codes from skew polynomial rings

$$(R_F, d_R) \cong (M_n(\mathbb{F}_{q^s}), d_R)$$

- n even
- q odd

$$\left\{ \alpha'_0 + \sum_{i=1}^{k-1} \alpha_i x^i + \gamma \alpha'_k x^k : \alpha_i \in \mathbb{F}_{q^n}, \alpha'_0, \alpha'_k \in \mathbb{F}_{q^{n/2}} \right\} \subseteq \frac{R}{R(x^n - 1)}$$

Codes from skew polynomial rings

$$(R_F, d_R) \cong (M_n(\mathbb{F}_{q^s}), d_R)$$

- n even
- q odd

$$\left\{\alpha'_0 + \sum_{i=1}^{k-1} \alpha_i x^i + \gamma\alpha'_k x^k : \alpha_i \in \mathbb{F}_{q^n}, \alpha'_0, \alpha'_k \in \mathbb{F}_{q^{n/2}}\right\} \subseteq \frac{R}{R(x^n - 1)}$$

Theorem (F.J. Lobillo, PS and J. Sheekey, 2025)

$$D(F) := \left\{\alpha'_0 + \sum_{i=1}^{sk-1} \alpha_i x^i + \gamma\alpha'_{sk} x^{sk} : \alpha_i \in \mathbb{F}_{q^n}, \alpha'_0, \alpha'_{sk} \in \mathbb{F}_{q^{n/2}}\right\} \subseteq R_F \cong M_n(\mathbb{F}_{q^s}).$$

Codes from skew polynomial rings

$$(R_F, d_R) \cong (M_n(\mathbb{F}_{q^s}), d_R)$$

- n even
- q odd

$$\left\{\alpha_0' + \sum_{i=1}^{k-1} \alpha_i x^i + \gamma\alpha_k' x^k : \alpha_i \in \mathbb{F}_{q^n}, \alpha_0', \alpha_k' \in \mathbb{F}_{q^{n/2}}\right\} \subseteq \frac{R}{R(x^n - 1)}$$

Theorem (F.J. Lobillo, PS and J. Sheekey, 2025)

$$D(F) := \left\{\alpha_0' + \sum_{i=1}^{sk-1} \alpha_i x^i + \gamma\alpha_{sk}' x^{sk} : \alpha_i \in \mathbb{F}_{q^n}, \alpha_0', \alpha_{sk}' \in \mathbb{F}_{q^{n/2}}\right\} \subseteq R_F \cong M_n(\mathbb{F}_{q^s}).$$

$$(-1)^{ks} F(0)^k \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\gamma) \notin \mathbb{F}_q^{(2)}$$

Codes from skew polynomial rings

$$(R_F, d_R) \cong (M_n(\mathbb{F}_{q^s}), d_R)$$

- n even
- q odd

$$\left\{ \alpha_0' + \sum_{i=1}^{k-1} \alpha_i x^i + \gamma \alpha_k' x^k : \alpha_i \in \mathbb{F}_{q^n}, \alpha_0', \alpha_k' \in \mathbb{F}_{q^{n/2}} \right\} \subseteq \frac{R}{R(x^n - 1)}$$

Theorem (F.J. Lobillo, PS and J. Sheekey, 2025)

$$D(F) := \left\{ \alpha_0' + \sum_{i=1}^{sk-1} \alpha_i x^i + \gamma \alpha_{sk}' x^{sk} : \alpha_i \in \mathbb{F}_{q^n}, \alpha_0', \alpha_{sk}' \in \mathbb{F}_{q^{n/2}} \right\} \subseteq R_F \cong M_n(\mathbb{F}_{q^s}).$$

$$(-1)^{ks} F(0)^k \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\gamma) \notin \mathbb{F}_q^{(2)}$$

$$\Downarrow$$

$D(F)$ is an MRD code in $M_n(\mathbb{F}_{q^s})$ with $|D(F)| = q^{nsk}$ and $d(D(F)) = n - k + 1$

Codes from skew polynomial rings

Theorem (F.J. Lobillo, PS, J. Sheekey 2025)

$$D(F) := \left\{ \alpha_0' + \sum_{i=1}^{sk-1} \alpha_i x^i + \gamma \alpha_{sk}' x^{sk} : \alpha_i \in \mathbb{F}_{q^n}, \alpha_0', \alpha_{sk}' \in \mathbb{F}_{q^{n/2}} \right\} \subseteq R_F \cong M_n(\mathbb{F}_{q^s}).$$

$$(-1)^{ks} F(0)^k \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\gamma) \notin \mathbb{F}_q^{(2)}$$

$$\Downarrow$$

$D(F)$ is an MRD code in $M_n(\mathbb{F}_{q^s})$ with $|D(F)| = q^{nsk}$ and $d(D(F)) = n - k + 1$

Corollary (F.J. Lobillo, PS and J. Sheekey, 2025)

For $k = 1$, for every s, $D(F)$ defines a semifield over $\mathbb{F}_q$, with $|D(F)| = q^{sn}$.

Codes from skew polynomial rings

$$(R_F, d_R) \cong (M_n(\mathbb{F}_{q^s}), d_R)$$

Theorem (F.J. Lobillo, PS, and J. Sheekey, 2025)

$$D(F) := \left\{ \alpha'_0 + \sum_{i=1}^{sk-1} \alpha_i x^i + \gamma \alpha'_k x^{sk} : \alpha_i \in \mathbb{F}_{q^n}, \alpha'_0, \alpha'_{sk} \in \mathbb{F}_{q^{n/2}} \right\} \subseteq R_F \cong M_n(\mathbb{F}_{q^s}).$$

$s = 1$ and $F(y) = y - 1$

$$D(F) = \left\{ \alpha'_0 + \sum_{i=1}^{k-1} \alpha_i x^i + \gamma \alpha'_k : \alpha_i \in \mathbb{F}_{q^n}, \alpha'_0, \alpha'_k \in \mathbb{F}_{q^{n/2}} \right\} \subseteq R_F = \frac{R}{R(x^n - 1)} \cong M_n(\mathbb{F}_q)$$

Trombetti-Zhou codes

Codes from skew polynomial rings

$$(R_F, d_R) \cong (M_n(\mathbb{F}_{q^s}), d_R)$$

Theorem (F.J. Lobillo, PS, J. Sheekey 2025)

$$D(F) := \left\{ \alpha_0' + \sum_{i=1}^{sk-1} \alpha_i x^i + \gamma \alpha_{sk}' x^{sk} : \alpha_i \in \mathbb{F}_{q^n}, \alpha_0', \alpha_{sk}' \in \mathbb{F}_{q^{n/2}} \right\} \subseteq R_F \cong M_n(\mathbb{F}_{q^s}).$$

$k = 1$, $F(y) = y - 1$ and $s = 1$

$$D(F) = \left\{ \alpha_0' + \gamma \alpha_1' : \alpha_0', \alpha_1' \in \mathbb{F}_{q^{n/2}} \right\} \subseteq R_F = \frac{R}{RF(x^n)} \cong M_n(\mathbb{F}_q)$$

Hughes-Kleinfeld semifields

Equivalence Issue

$(\mathbb{A}, +, \star)$ semifield

$$\mathbb{N}_l(\mathbb{A}) = \{a \in \mathbb{A} : a \star (b \star c) = (a \star b) \star c, \text{ for all } b, c \in \mathbb{A}\}$$

(Left nucleus)

$$\mathbb{N}_m(\mathbb{A}) = \{b \in \mathbb{A} : a \star (b \star c) = (a \star b) \star c, \text{ for all } a, c \in \mathbb{A}\},$$

(Middle nucleus)

$$\mathbb{N}_r(\mathbb{A}) = \{c \in \mathbb{A} : a \star (b \star c) = (a \star b) \star c, \text{ for all } a, b \in \mathbb{A}\},$$

(Right nucleus)

$$Z(\mathbb{A}) = \mathbb{N}_l(\mathbb{A}) \cap \mathbb{N}_m(\mathbb{A}) \cap \mathbb{N}_r(\mathbb{A}) \cap \{a \in \mathbb{A} : a \star b = b \star a \text{ for all } b \in \mathbb{A}\}.$$

(center)

Equivalence Issue

$\mathcal{C} \subseteq M_n(\mathbb{F})$

$$L(\mathcal{C}) = \{A \in M_n(\mathbb{F}) : A\mathcal{C} \subseteq \mathcal{C}\}$$

(Left idealiser)

$$R(\mathcal{C}) = \{B \in M_n(\mathbb{F}) : \mathcal{C}B \subseteq \mathcal{C}\},$$

(Right idealiser)

$$Cen(\mathcal{C}) = \{A \in M_n(\mathbb{F}) : AX = XA \text{ for every } X \in \mathcal{C}\},$$

(centraliser)

$$Z(\mathcal{C}) = L(\mathcal{C}) \cap C(\mathcal{C}).$$

(center)

Equivalence Issue

Theorem (G. Lunardon, R. Trombetti, and Y. Zhou, 2017- J. Sheekey, 2020)

- $(\mathbb{A}, +, \star)$ semifield, $\mathcal{C} = \mathcal{C}(\mathbb{A})$ spread set. Then

$$|L(\mathcal{C})| = |\mathbb{N}_l(\mathbb{A})|$$

$$|R(\mathcal{C})| = |\mathbb{N}_m(\mathbb{A})|$$

$$|Cen(\mathcal{C})| = |\mathbb{N}_r(\mathbb{A})|$$

$$|Z(\mathcal{C})| = |Z(\mathbb{A})|$$

- $I_n \in \mathcal{C}, \mathcal{C}' \subseteq M_n(\mathbb{F}_q)$. If $\mathcal{C} \sim \mathcal{C}'$, then

$$|L(\mathcal{C})| = |L(\mathcal{C}')|$$

$$|R(\mathcal{C})| = |R(\mathcal{C}')|$$

$$|Cen(\mathcal{C})| = |Cen(\mathcal{C}')|$$

$$|Z(\mathcal{C})| = |Z(\mathcal{C}')|$$

Equivalence Issue

Theorem (G. Lunardon, R. Trombetti, and Y. Zhou, 2017- J. Sheekey, 2020)

- $(\mathbb{A}, +, \star)$ semifield, $\mathcal{C} = \mathcal{C}(\mathbb{A})$ spread set. Then

$$|L(\mathcal{C})| = |\mathbb{N}_l(\mathbb{A})|$$

$$|R(\mathcal{C})| = |\mathbb{N}_m(\mathbb{A})|$$

$$|Cen(\mathcal{C})| = |\mathbb{N}_r(\mathbb{A})|$$

$$|Z(\mathcal{C})| = |Z(\mathbb{A})|$$

- $I_n \in \mathcal{C}, \mathcal{C}' \subseteq M_n(\mathbb{F}_q)$. If $\mathcal{C} \sim \mathcal{C}'$, then

$$(|\mathcal{C}|, |L(\mathcal{C})|, |R(\mathcal{C})|, |Cen(\mathcal{C})|, |Z(\mathcal{C})|)$$

Nuclear parameters of $\mathcal{C}$

$$|Cen(\mathcal{C})| = |Cen(\mathcal{C}')|$$

$$|Z(\mathcal{C})| = |Z(\mathcal{C}')|$$

Equivalence Issue

Theorem (F.J. Lobillo, PS, and J. Sheekey, 2025)

$\mathcal{C} = D(F)$, $k \leq n/2$. Then

$$L(\mathcal{C}) \cong \mathbb{F}_{q^{n/2}} \quad R(\mathcal{C}) \cong \mathbb{F}_{q^{n/2}} \quad Cen(\mathcal{C}) \cong \mathbb{F}_{q^s} \quad Z(\mathcal{C}) \cong \mathbb{F}_q$$

Equivalence Issue

Theorem (F.J. Lobillo, PS, and J. Sheekey, 2025)

$\mathcal{C} = D(F)$, $k \leq n/2$. Then

$$L(\mathcal{C}) \cong \mathbb{F}_{q^{n/2}} \quad R(\mathcal{C}) \cong \mathbb{F}_{q^{n/2}} \quad Cen(\mathcal{C}) \cong \mathbb{F}_{q^s} \quad Z(\mathcal{C}) \cong \mathbb{F}_q$$

Theorem (F.J. Lobillo, PS, and J. Sheekey, 2025)

The family $D(F)$ contains new semifields and new MRD codes for infinite choices of s and n.

What's next?

Why $F(y)$ irreducible?!

What's next?

Why $F(y)$ irreducible?!

$$F(y) = F_1(y) \cdots F_t(y), \quad \gcd(F_i, F_j) = 1$$

F_i irreducible polynomial

What's next?

Why $F(y)$ irreducible?!

$$F(y) = F_1(y)\cdots F_t(y), \quad \gcd(F_i, F_j) = 1$$

F_i irreducible polynomial

$$\Downarrow$$

$$\frac{R}{RF(x^n)} \cong \bigoplus_{i=1}^{t} \frac{R}{RF_i(x^n)} \cong \bigoplus_{i=1}^{t} M_n(\mathbb{F}_{q^{s_i}}), \quad s_i = \deg(F_i).$$

What's next?

Why $F(y)$ irreducible?!

$$F(y) = F_1(y)\cdots F_t(y), \quad \gcd(F_i, F_j) = 1$$

F_i irreducible polynomial

$$\Downarrow$$

$$\frac{R}{RF(x^n)} \cong \bigoplus_{i=1}^{t} \frac{R}{RF_i(x^n)} \cong \bigoplus_{i=1}^{t} M_n(\mathbb{F}_{q^{s_i}}), \quad s_i = \deg(F_i).$$

$$\Downarrow$$

$$\left(\frac{R}{RF(x^n)}, \mathrm{srk}\right) \cong \left(\bigoplus_{i=1}^{t} M_n(\mathbb{F}_{q^{s_i}}), \mathrm{srk}\right)$$

What's next?

Why $F(y)$ irreducible?!

$$F(y) = F_1(y)\cdots F_t(y), \quad \gcd(F_i, F_j) = 1$$

F_i irreducible polynomial

$$\Downarrow$$

A. Neri and PS: Sum-rank metric codes and additive MDS codes from quotients of skew polynomial rings, *in preparation.*

New constructions of MSRD codes and additive MDS codes

$$\left(\frac{R}{RF(x^n)}, \mathrm{srk}\right) \cong \left(\bigoplus_{i=1}^{t} M_n(\mathbb{F}_{q^{s_i}}), \mathrm{srk}\right)$$

What's next?

$$F(y) = F_1(y)\cdots F_t(y), \quad \gcd(F_i, F_j) = 1$$

$$F_i \text{ irreducible polynomial }, \ deg(F_i) = s$$

$$\left(\frac{R}{RF(x^n)}, \mathrm{srk}\right) \cong \left(\bigoplus_{i=1}^{t} M_n(\mathbb{F}_{q^s}), \mathrm{srk}\right)$$

Theorem (A. Neri, and PS)

Let $a \in R/RF(x^n)$. Then

$$\mathrm{srk}(a) = tn - \frac{1}{s}\deg(\mathrm{gcrd}(a, F(x^n)))$$

What's next?

$$\left(\frac{R}{RF(x^n)}, \mathrm{srk}\right) \cong \left(\bigoplus_{i=1}^{t} M_n(\mathbb{F}_{q^s}), \mathrm{srk}\right)$$

Theorem (A. Neri, and PS)

$$S(F) := \left\{\alpha_0 + \sum_{i=1}^{sk-1} \alpha_i x^i + \eta\rho(\alpha_0)x^{sk} : \alpha_i \in \mathbb{F}_{q^n}\right\} \subseteq R_F \cong \bigoplus_{i=1}^{t} M_n(\mathbb{F}_{q^s})$$

What's next?

$$\left(\frac{R}{RF(x^n)}, \mathrm{srk}\right) \cong \left(\bigoplus_{i=1}^{t} M_n(\mathbb{F}_{q^s}), \mathrm{srk}\right)$$

Theorem (A. Neri, and PS)

$$S(F) := \left\{\alpha_0 + \sum_{i=1}^{sk-1} \alpha_i x^i + \eta\rho(\alpha_0)x^{sk} : \alpha_i \in \mathbb{F}_{q^n}\right\} \subseteq R_F \cong \bigoplus_{i=1}^{t} M_n(\mathbb{F}_{q^s})$$

$$\mathbb{N}_{\mathbb{F}_{q^n}/\mathbb{K}'}(\eta)\mathbb{N}_{\mathbb{F}_q/\mathbb{K}'}\left((-1)^{sk(n-1)}\prod_{i=1}^{t} F_{i,0}^{j_i}\right) \neq 1, \quad \text{with} \quad j_1 + \cdots + j_t = k$$

What's next?

$$\left(\frac{R}{RF(x^n)}, \mathrm{srk}\right) \cong \left(\bigoplus_{i=1}^{t} M_n(\mathbb{F}_{q^s}), \mathrm{srk}\right)$$

Theorem (A. Neri, and PS)

$$S(F) := \left\{\alpha_0 + \sum_{i=1}^{sk-1} \alpha_i x^i + \eta\rho(\alpha_0)x^{sk} : \alpha_i \in \mathbb{F}_{q^n}\right\} \subseteq R_F \cong \bigoplus_{i=1}^{t} M_n(\mathbb{F}_{q^s})$$

$$\mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{K}'}(\eta)\mathrm{N}_{\mathbb{F}_q/\mathbb{K}'}\left((-1)^{sk(n-1)} \prod_{i=1}^{t} F_{i,0}^{j_i}\right) \neq 1, \quad \text{with} \quad j_1 + \cdots + j_t = k$$

$$\Downarrow$$

$S(F)$ is an MSRD code in $\bigoplus_{i=1}^{t} M_n(\mathbb{F}_{q^s})$ with $d(S(F)) = tn - k + 1$

U. Martínez-Peñas: Skew and linearized Reed-Solomon codes and maximum sum rank distance codes over any division ring. *Journal of Algebra*, (2018) (LRS codes)

A. Neri: Twisted linearized Reed-Solomon codes: A skew polynomial framework. *Journal of Algebra*, (2022) (TLRS codes)

What's next?

$$\left(\frac{R}{RF(x^n)}, \mathrm{srk}\right) \cong \left(\bigoplus_{i=1}^{t} M_n(\mathbb{F}_{q^s}), \mathrm{srk}\right)$$

Theorem (A. Neri, and PS, 2025)

$$D(F) := \left\{\alpha_0' + \sum_{i=1}^{sk-1} \alpha_i x^i + \gamma \alpha_{sk}' x^{sk} : \alpha_i \in \mathbb{F}_{q^n}, \alpha_0', \alpha_{sk}' \in \mathbb{F}_{q^{n/2}}\right\} \subseteq R_F \cong M_n(\mathbb{F}_{q^s}).$$

What's next?

$$\left(\frac{R}{RF(x^n)}, \mathrm{srk}\right) \cong \left(\bigoplus_{i=1}^{t} M_n(\mathbb{F}_{q^s}), \mathrm{srk}\right)$$

Theorem (A. Neri, and PS, 2025)

$$D(F) := \left\{\alpha_0' + \sum_{i=1}^{sk-1} \alpha_i x^i + \gamma\alpha_{sk}' x^{sk} : \alpha_i \in \mathbb{F}_{q^n}, \alpha_0', \alpha_{sk}' \in \mathbb{F}_{q^{n/2}}\right\} \subseteq R_F \cong M_n(\mathbb{F}_{q^s}).$$

$$(-1)^{sk(n-1)} \prod_{i=1}^{t} F_{i,0}^{j_i} \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\gamma) \notin \mathbb{F}_q^{(2)}, \quad \text{with } \; j_1 + \cdots + j_t = k.$$

What's next?

$$\left(\frac{R}{RF(x^n)}, \mathrm{srk}\right) \cong \left(\bigoplus_{i=1}^{t} M_n(\mathbb{F}_{q^s}), \mathrm{srk}\right)$$

Theorem (A. Neri, and PS, 2025)

$$D(F) := \left\{\alpha'_0 + \sum_{i=1}^{sk-1} \alpha_i x^i + \gamma \alpha'_{sk} x^{sk} : \alpha_i \in \mathbb{F}_{q^n}, \alpha'_0, \alpha'_{sk} \in \mathbb{F}_{q^{n/2}}\right\} \subseteq R_F \cong M_n(\mathbb{F}_{q^s}).$$

$$(-1)^{sk(n-1)} \prod_{i=1}^{t} F_{i,0}^{j_i} \mathrm{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(\gamma) \notin \mathbb{F}_q^{(2)}, \quad \text{with} \quad j_1 + \cdots + j_t = k.$$

$$\Downarrow$$

$D(F)$ is an MSRD code in $\bigoplus_{i=1}^{t} M_n(\mathbb{F}_{q^s})$ with $d(D(F)) = tn - k + 1$

A. Neri: Twisted linearized Reed-Solomon codes: A skew polynomial framework. *Journal of Algebra*, (2022) (TLRS codes of TZ-type)

Thank you for your attention!