Matrici, Polinomi non Commutativi e Teoria dei Codici

Seminario UMI Crittografia e Codici – De Cifris

Alessandro Neri

6 Ottobre 2021

Contents

Part 1:
Background, History & Motivations

Coding Theory

"Coding theory is the theory of subsets (subspaces) of a metric space"

- (Finite) field $\mathbb{K}$.
- V finite dimensional $\mathbb{K}$-vector space.
- $\delta : V \times V \to \mathbb{R}_{\geq 0}$ **distance** function.
- (V, δ) **metric space**.

A $[V, k, d]$ **code** $\mathcal{C}$ is a k-dimensional $\mathbb{K}$-subspace of V endowed with the metric δ. The parameter d is known as the **minimum distance** of $\mathcal{C}$, that is

$$d := \min\{\delta(u, v) \mid u, v \in \mathcal{C}, u \neq v.\}.$$

Coding Theory Examples

1. Hamming-metric codes
   - $V = \mathbb{K}^\ell$.
   - $\delta = \delta_{\mathsf{H}}$ the Hamming distance on $\mathbb{K}^\ell$ defined as

$$\delta_{\mathsf{H}}(u, v) = \mathrm{wt}_{\mathsf{H}}(u - v) := \#\{i \mid (u - v)_i \neq 0\}.$$

2. Rank-metric codes
   - $V = \mathrm{Mat}_m(\mathbb{K})$.
   - $\delta = \delta_{\mathsf{R}}$ the rank distance on $\mathrm{Mat}_m(\mathbb{K})$ defined as

$$\delta_{\mathsf{R}}(A, B) := \mathrm{rk}(A - B).$$

3. Sum-rank-metric codes
   - $V = (\mathrm{Mat}_m(\mathbb{K}))^\ell$.
   - $\delta = \delta_{\mathsf{SR}}$ the sum-rank distance on $(\mathrm{Mat}_m(\mathbb{K}))^\ell$ defined as

$$\begin{aligned}\delta_{\mathsf{SR}}((A_1, \ldots, A_\ell), (B_1, \ldots, B_\ell)) &= \mathrm{wt}_{\mathsf{SR}}(A_1 - B_1, \ldots, A_\ell - B_\ell) \\ &:= \sum_{i=1}^{\ell} \mathrm{rk}(A_i - B_i).\end{aligned}$$

Matrices with Restricted Entries

- (Finite) field $\mathbb{K}$.
- ℓ, m, n positive integers with $n = \ell m$.
- $S \subseteq [n] \times [n]$ $\qquad [n] := \{1, \ldots, n\}$

$$\mathsf{Mat}_n^S(\mathbb{K}) := \{A \in \mathsf{Mat}_n(\mathbb{K}) \mid a_{ij} = 0 \; \forall (i,j) \notin S\}$$

It is the subspace generated by the standard basis elements E_{ij} for $(i,j) \in S$.

Main Questions

Question 1

For a given d, determine the maximum value k such that there exists a $\mathbb{K}$-subspace of $\mathsf{Mat}_n^S(\mathbb{K})$ whose nonzero elements have all rank at least d, that is

$$\kappa(n, d, S, \mathbb{K}) := \max\left\{\dim_{\mathbb{K}}(\mathcal{C}) \mid \mathcal{C} \subseteq \mathsf{Mat}_n^S(\mathbb{K}), \mathrm{rk}(A) \geq d \; \forall A \in \mathcal{C} \setminus \{0\}\right\}$$

Question 2

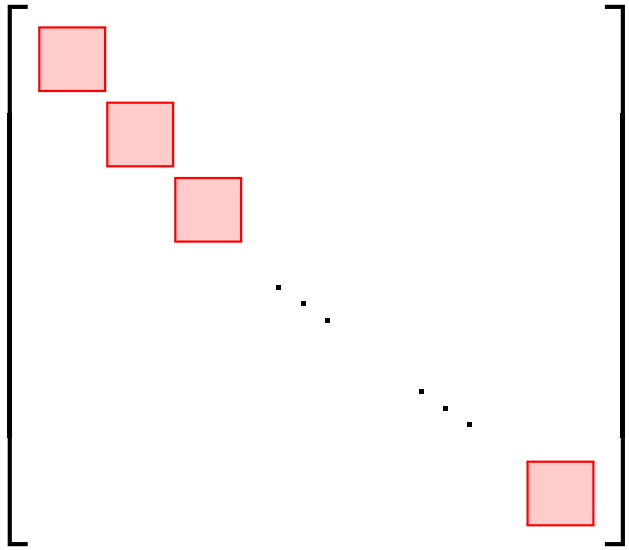
Find a concrete construction of a space $\mathcal{C} \subseteq \mathsf{Mat}_n^S(\mathbb{K})$ such that $\mathrm{rk}(A) \geq d$ for all $A \in \mathcal{C} \setminus \{0\}$ with $\dim_{\mathbb{K}}(\mathcal{C}) = \kappa(n, d, S, \mathbb{K})$.

Motivations

- Coding theory, network coding, distributed storage.
- Cryptography.
- Linear (tensor) rank preservers.
- Finite semifields.
- Linear sets in finite geometry.
- Tensor decomposition.
- q-analogues theory (e.g. q-permutations).
- Differential topology.
- Clifford algebras.
- ...

Coding Theoretic Meaning of κ: Hamming metric

$$S := \{(i, i) \mid i \in [n]\},$$

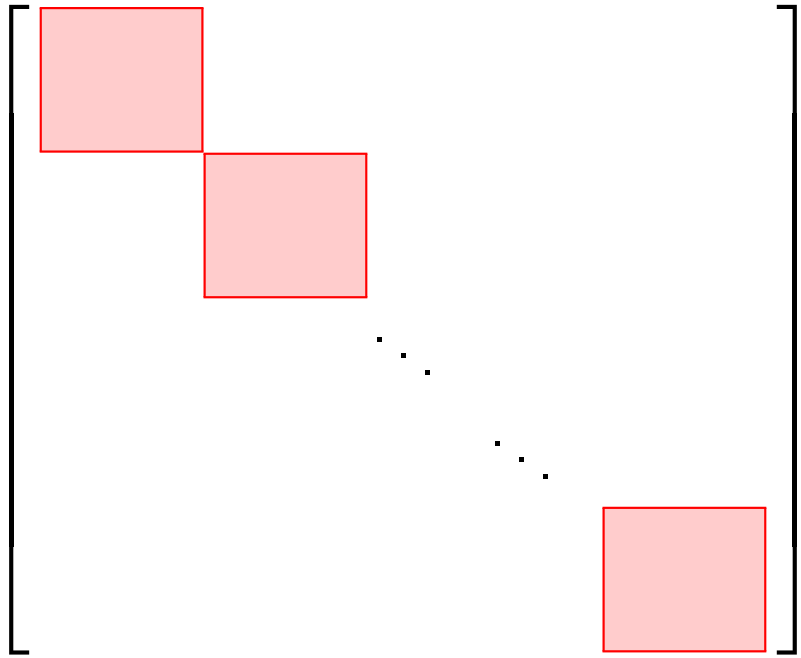


Coding Theoretic Meaning of κ: Rank Metric

$$S := [n] \times [n],$$

Coding Theoretic Meaning of κ: Sum-Rank Metric

$$S_{\ell,m} := \bigcup_{i=1}^{\ell} ([im] \setminus [(i-1)m])^2,$$



Bounds from Coding Theory

For $S = S_{\ell,m}$, Question 1 and Question 2 concern optimal codes in the sum-rank metric (maximum dimension, construction)

- $(\mathrm{Mat}_n^{S_{1,m}}(\mathbb{K}), \mathrm{rk}) = (\mathrm{Mat}_m(\mathbb{K}), \mathrm{rk})$, **rank metric**
- $(\mathrm{Mat}_n^{S_{\ell,1}}(\mathbb{K}), \mathrm{rk}) \cong (\mathbb{K}^\ell, \mathrm{wt_H})$ **Hamming metric**

Theorem (Singleton-like bound)

$$\kappa(n, d, S_{\ell,m}, \mathbb{K}) \leq m(\ell m - d + 1).$$

Sharpness of the Singleton-like bound

Question 1bis

When is the Singleton-like bound sharp?

1. If $\ell = 1$ and $\mathbb{K} = \overline{\mathbb{K}}$ is algebraically closed, then

$$\kappa(n, d, S_{1,n}, \overline{\mathbb{K}}) = (n - d + 1)^2.$$


R. Westwick, Spaces of linear transformations of equal rank, 1972. Upper bound


R. M. Roth, Maximum-rank array codes and their application to crisscross error correction, 1991. Construction


E. G. Rees, Linear spaces of real matrices of large rank, 1996. Generalization to the rectangular case

Sharpness of the Singleton-like bound

Question 1bis

When is the Singleton-like bound sharp?

2. If $m = 1$, then we have the **MDS Conjecture**: If $3 \leq d \leq n-1$, then

$$\kappa(n, d, S_{n,1}, \mathbb{K}) = n - d + 1$$

if and only if $|\mathbb{K}| \geq n - 1$ or $d \in \{4, 2^h - 1\}$ and $|\mathbb{K}| = 2^h = n - 2$.

B. Segre, Curve razionali normali e k-archi negli spazi finiti, 1955. Conjecture

I. Reed, G. Solomon, Polynomial codes over certain finite fields, 1960. Construction

Sharpness of the Singleton-like bound

Question 1bis

When is the Singleton-like bound sharp?

3. If $\ell = 1$ and $\mathbb{K} = \mathbb{R}$, then

$$\kappa(n, n, S_{1,n}, \mathbb{R}) = \rho(n),$$

Write

$$n = 2^a b, \ b \text{ odd}$$
$$a = 4c + d$$
$$0 \leq d \leq 3$$

then $\rho(n) = 2^c + 8d$ is the n-th **Radon-Hurwitz number**

I. M. James, Whitehead products and vector-fields on spheres, 1957. Construction

J. F. Adams, Vector Fields on Spheres, 1962. Upper Bound

Sharpness of the Singleton-like bound

Question 1bis

When is the Singleton-like bound sharp?

4. If $\ell = 1$ and $\mathbb{K} = \mathbb{F}_q$, then

$$\kappa(n, d, S_{1,n}, \mathbb{F}_q) = n(n - d + 1),$$

This is given by **Delsarte-Gabidulin codes**.

P. Delsarte, Bilinear forms over a finite field, with applications to coding theory, 1978.

E. M. Gabidulin, Theory of codes with maximum rank distance, 1985.

Sharpness of the Singleton-like bound

Question 1bis

When is the Singleton-like bound sharp?

4. If $\ell = 1$ and $\mathbb{K}$ s.t. $\exists\, \mathbb{L}/\mathbb{K}$ cyclic of degree n, then

$$\kappa(n, d, S_{1,n}, \mathbb{K}) = n(n - d + 1),$$

This is given by **Delsarte-Gabidulin codes**.


P. Delsarte, Bilinear forms over a finite field, with applications to coding theory, 1978.


E. M. Gabidulin, Theory of codes with maximum rank distance, 1985.


R. M. Guralnick, Invertible preservers and algebraic groups, 1994.

Skew Polynomials

Let $\sigma \in \mathrm{Aut}(\mathbb{L})$. Consider

- $\mathbb{L}[X;\sigma] = \{a_0 + a_1X + \ldots + a_tX^t \mid a_i \in \mathbb{L}, t \in \mathbb{N}\}$,
- $+$ is the usual addition on polynomials,
- $\cdot$ follows the rule

$$X \cdot a := \sigma(a)X, \qquad \forall\, a \in \mathbb{L}.$$

Properties

(1) $(\mathbb{L}[X;\sigma], +, \cdot)$ is a noncommutative ring, called **ring of skew polynomials**.

(2) $(\mathbb{L}[X;\sigma], +, \cdot)$ is a left Euclidean ring. There exists **greatest common right divisor (gcrd)** and **least common left multiple (lclm)** of two skew polynomials.

(3) The center of $\mathbb{L}[X;\sigma]$ is $\mathbb{L}^{\sigma}[X^{\mathrm{ord}(\sigma)}]$ (if $\mathrm{ord}(\sigma) < \infty$).

Main Algebra Isomorphism: Rank-Metric Codes

Theorem

- $\langle \sigma \rangle = \mathsf{Gal}(\mathbb{L}/\mathbb{K})$,
- $\mathsf{ord}(\sigma) = m = [\mathbb{L} : \mathbb{K}]$.

Then

$$\mathbb{L}[X;\sigma]/(X^m - 1) \cong \mathsf{End}_{\mathbb{K}}(\mathbb{L}) \cong \mathsf{Mat}_m(\mathbb{K}),$$

as $\mathbb{K}$-algebras.

$$\sum_{i=0}^{t} a_i X^i \longmapsto \left(\beta \longmapsto \sum_{i=0}^{t} a_i \sigma^i(\beta) \right) =: \mathsf{ev}_\beta(P).$$

S. U. Chase, D. K. Harrison, and A. Rosenberg, Galois theory and cohomology of commutative rings, 1969.

Bounding the Rank of Skew Polynomials

For every $P(X) \in \mathbb{L}[X;\sigma]/(X^m - 1)$, we can define its **kernel** as

$$\ker(P) := \{\beta \in \mathbb{L} \mid \mathrm{ev}_\beta(P) = 0\},$$

and its **rank** as $\mathbb{K}$-linear map.

Theorem (Delsarte '78, Guralnick '94)

1. $\ker(P) = \ker(\mathrm{gcrd}(P(X), X^m - 1))$,
2. $\dim_{\mathbb{K}}(\ker(P)) = \deg(\mathrm{gcrd}(P(X), X^m - 1))(\leq \deg(P(X))$.

$$\mathcal{G}_{d,\sigma} := \left\{ P(X) \in \mathbb{L}[X;\sigma]/(X^m - 1) \mid \deg P(X) < m - d + 1 \right\}.$$

Delsarte-Gabidulin Code

- $\dim_{\mathbb{K}}(\mathcal{G}_{d,\sigma}) = m(m - d + 1)$,
- $\mathrm{rk}(P) \geq d$.

Part 2:
Skew Polynomial Setting for Sum-Rank Metric

A. Neri, Twisted linearized Reed-Solomon codes: A skew polynomial framework, arXiv:2105.10451, 2021.

Setting

Lemma

For every $P(X) \in \mathbb{L}[X;\sigma]$, and every $\alpha \in \mathbb{L}$, the map

$$P(X) \longmapsto P_\alpha(X) := P(\alpha X)$$

is a $\mathbb{K}$-algebra isomorphism.

From now on we fix

- $\langle \sigma \rangle = \mathsf{Gal}(\mathbb{L}/\mathbb{K})$,
- $\alpha_1, \ldots, \alpha_\ell \in \mathbb{L}^*$,
- $\mathbf{N}_{\mathbb{L}/\mathbb{K}}(\alpha_1) = \lambda_1, \ldots, \mathbf{N}_{\mathbb{L}/\mathbb{K}}(\alpha_\ell) = \lambda_\ell \in \mathbb{K}^*$ pairwise distinct.
- $H_\lambda(X) := \prod_{i=1}^{\ell}(X^m - \lambda_i)$.

Main Algebra Isomorphisms: Sum-Rank-Metric Codes

Theorem (N. 2021)

- $\alpha_1, \ldots, \alpha_\ell \in \mathbb{L}^*$,
- $\mathbf{N}_{\mathbb{L}/\mathbb{K}}(\alpha_1) = \lambda_1, \ldots, \mathbf{N}_{\mathbb{L}/\mathbb{K}}(\alpha_\ell) = \lambda_\ell \in \mathbb{K}^*$ pairwise distinct.
- $H_\lambda(X) := \prod_{i=1}^{\ell}(X^m - \lambda_i)$.

Then, **as $\mathbb{K}$-algebras**,

$$\mathbb{L}[X;\sigma]_{/(H_\lambda(X))} \cong \left(\mathbb{L}[X;\sigma]_{/(X^m-1)}\right)^\ell \cong \mathrm{Mat}_n^{S_{\ell,m}}(\mathbb{K}).$$

$$P(X) \longmapsto (\overline{P}_{\alpha_1}(X), \ldots, \overline{P}_{\alpha_\ell}(X)).$$

$$\mathrm{wt_{SR}}(P) := \sum_{i=1}^{\ell} \mathrm{rk}(\overline{P}_{\alpha_i}) = n - \sum_{i=1}^{\ell} \dim_{\mathbb{K}}(\ker(\overline{P}_{\alpha_i})).$$

Main Algebra Isomorphisms: Hamming-Metric Codes

Theorem

- $\alpha_1, \ldots, \alpha_\ell \in \mathbb{K}^*$,
- $\alpha_1 = \lambda_1, \ldots, \alpha_\ell = \lambda_\ell \in \mathbb{K}^*$ pairwise distinct.
- $H_\lambda(X) := \prod_{i=1}^{\ell}(X - \lambda_i)$.

Then, **as $\mathbb{K}$-algebras**,

$$K[X]/(H_\lambda(X)) \cong \left(\mathbb{K}[X]/(X-1)\right)^\ell \cong \mathsf{Mat}_\ell^{S_{\ell,1}}(\mathbb{K}) \cong \mathbb{K}^\ell.$$

$$\begin{aligned} P(X) \longmapsto & (\overline{P}_{\alpha_1}(X), \ldots, \overline{P}_{\alpha_\ell}(X)) \\ = & (P(\lambda_1), \ldots, P(\lambda_\ell)). \end{aligned}$$

Example I

- $\mathbb{L} = \mathbb{F}_{5^3}$, $\sigma(\alpha) = \alpha^5$ ($m = 3$, $\mathbb{K} = \mathbb{F}_5$), $\ell = 4$.
- γ primitive element of $\mathbb{L}$, root of $y^3 + 3y + 3$.
- $\alpha_i = i$ for $i = 1, 2, 3, 4$.
- $\lambda_1 = 1$, $\lambda_2 = 3$, $\lambda_3 = 2$, $\lambda_4 = 4$.
- $H_\lambda(X) = \prod_i (X^3 - i) = X^{12} - 1$.
- $\boxed{P(X) = X^4 + 2X^3 + 3X^2 + 3X + 1}$

$$P_1(X) = P(1 \cdot X) = P(X)$$
$$\overline{P}_1(X) = P(X) \mod (X^3 - 1) = 3X^2 + 4X + 3$$

Example I

- $\mathbb{L} = \mathbb{F}_{5^3}$, $\sigma(\alpha) = \alpha^5$ ($m = 3$, $\mathbb{K} = \mathbb{F}_5$), $\ell = 4$.
- γ primitive element of $\mathbb{L}$, root of $y^3 + 3y + 3$.
- $\alpha_i = i$ for $i = 1, 2, 3, 4$.
- $\lambda_1 = 1$, $\lambda_2 = 3$, $\lambda_3 = 2$, $\lambda_4 = 4$.
- $H_\lambda(X) = \prod_i (X^3 - i) = X^{12} - 1$.
- $\boxed{P(X) = X^4 + 2X^3 + 3X^2 + 3X + 1}$

$$P_2(X) = P(2 \cdot X) = (2X)^4 + 2(2X)^3 + 3(2X)^2 + 3(2X) + 1$$
$$\overline{P}_2(X) = P(2X) \mod (X^3 - 1) = 2X^2 + 2X + 2$$

Example I

- $\mathbb{L} = \mathbb{F}_{5^3}$, $\sigma(\alpha) = \alpha^5$ ($m = 3$, $\mathbb{K} = \mathbb{F}_5$), $\ell = 4$.
- γ primitive element of $\mathbb{L}$, root of $y^3 + 3y + 3$.
- $\alpha_i = i$ for $i = 1, 2, 3, 4$.
- $\lambda_1 = 1$, $\lambda_2 = 3$, $\lambda_3 = 2$, $\lambda_4 = 4$.
- $H_\lambda(X) = \prod_i (X^3 - i) = X^{12} - 1$.
- $P(X) = X^4 + 2X^3 + 3X^2 + 3X + 1$

$$\overline{P}_1(X) = 3X^2 + 4X + 3, \quad \overline{P}_2(X) = 2X^2 + 2X + 2,$$
$$\overline{P}_3(X) = 2X^2, \quad \overline{P}_4(X) = 3X^2 + 3X + 4.$$

Example II

$$\overline{P}_1(X)=3X^2+4X+3, \quad \overline{P}_2(X)=2X^2+2X+2,$$
$$\overline{P}_3(X)=2X^2, \quad \overline{P}_4(X)=3X^2+3X+4.$$

$\mathcal{B}=(1,\gamma,\gamma^2)$ $\mathbb{K}$-basis of $\mathbb{L}$.

$$P(X) \longmapsto (\overline{P}_1(X), \overline{P}_2(X), \overline{P}_3(X), \overline{P}_4(X)) \downarrow_{\mathcal{B}}$$

$$\left(\begin{pmatrix} 040 \\ 042 \\ 020 \end{pmatrix}, \begin{pmatrix} 103 \\ 000 \\ 000 \end{pmatrix}, \begin{pmatrix} 222 \\ 001 \\ 013 \end{pmatrix}, \begin{pmatrix} 002 \\ 010 \\ 001 \end{pmatrix} \right).$$

$$\mathrm{wt_{SR}}(P) = 2 + 1 + 3 + 2 = 8$$

Bounding the Sum-Rank of a Skew Polynomial

Theorem

$$\sum_{i=1}^{\ell} \dim(\ker(\overline{P}_{\alpha_i}(X))) = \deg(\operatorname{gcrd}(P(X), H_\lambda(X)) \leq \deg(P(X)).$$

X. Caruso, Residues of skew rational functions and linearized Goppa codes, 2019.

$$\mathcal{L}_{d,\sigma} = \left\{ P(X) \in {}^{\mathbb{L}[X;\sigma]}\!/_{(H_\lambda(X))} \mid \deg(P(X)) < n-d+1 \right\}$$

Linearized Reed-Solomon Code

- $\dim_{\mathbb{K}}(\mathcal{L}_{d,\sigma}) = m(n-d+1)$,
- $\mathrm{wt}_{\mathrm{SR}}(P) \geq d$.

U. Martìnez-Penas, Skew and linearized Reed-Solomon codes and maximum sum rank distance codes over any division ring, 2018.

Sharpness of the Singleton-like bound

Question 1bis

When is the Singleton-like bound sharp?

5. If $\mathbb{K}$ is s.t. $\exists \mathbb{L}/\mathbb{K}$ cyclic of degree m and $|\mathbb{K}| \geq \ell + 1$, then

$$\kappa(n, d, S_{\ell,m}, \mathbb{K}) = m(n - d + 1),$$

This is given by **Linearized Reed-Solomon codes**.

Question 3

Is this the natural generalization of the MDS conjecture?

Extremal Skew Polynomials

For which polynomials does the bound is actually an equality?

$$\sum_{i=1}^{\ell} \dim(\ker(\overline{P}_{\alpha_i}(X))) = \deg(P(X))$$

$$\mathrm{wt}_{\mathrm{SR}}(P) = n - \deg(P(X))$$

For $P(X) = a_0 + a_1 X + \ldots + a_t X^t$, $a_t \neq 0$, consider its **Companion matrix** $C_P \in \mathrm{Mat}_t(\mathbb{L})$, and define

$$A_P := C_P \cdot \sigma(C_P) \cdot \ldots \cdot \sigma^{m-1}(C_P) \in \mathrm{Mat}_t(\mathbb{L}).$$


B. Csajbók, G. Marino, O. Polverino, and F. Zullo, A characterization of linearized polynomials with maximum kernel, 2019.


G. McGuire and J. Sheekey, A characterization of the number of roots of linearized and projective polynomials in the field of coefficients, 2019.

Main Theorem

Theorem (N. 2021)

Let $P(X) \in \mathbb{L}[X;\sigma]$ be a nonzero skew polynomial, and let $\{\alpha_1, \ldots, \alpha_\ell\} \subseteq \mathbb{L}^*$ be a set whose elements have pairwise distinct norms $\{\lambda_1, \ldots, \lambda_\ell\}$. The following are equivalent:

1. $\sum_{i=1}^{\ell} \dim \ker(P_{\alpha_i}) = \deg(P)$.
2. A_P is diagonalizable over $\mathbb{L}$ and its eigenvalues belong to $\{\lambda_1, \ldots, \lambda_\ell\}$.
3. $P(X)$ right-divides the skew polynomial $H_\lambda(X)$.

In the previous example:

- $\mathrm{wt}_{\mathrm{SR}}(P) = 8 = 12 - \deg(P(X))$,
- Eigenvalues of A_P are $\{\{1, 3, 3, 4\}\}$,
- $P(X) = X^4 + 2X^3 + 3X^2 + 3X + 1$ right divides $H_\lambda(X) = X^{12} - 1$.

Twisted Linearized Reed-Solomon Codes

Let $\eta \in \mathbb{L}$ such that $(-1)^{(\ell m-d+1)m}\mathbf{N}_{\mathbb{L}/\mathbb{K}}(\eta) \notin \langle \lambda_1, \ldots, \lambda_\ell \rangle$.

$$\mathcal{L}_{d,\sigma}(\eta, h) := \left\{ P(X) \in {}^{\mathbb{L}[X;\sigma]}\!/_{(H_\lambda(X))} \mid \begin{array}{l} \deg(P(X)) \leq n-d+1, \\ a_{n-d+1} = \sigma^h(a_0) \end{array} \right\}$$

Twisted Linearized Reed-Solomon Code

- $\dim_{\mathbb{K}}(\mathcal{L}_{d,\sigma}(\eta, h)) = m(n-d+1)$,
- $\mathrm{wt}_{\mathrm{SR}}(P) \geq d$.

For $\ell = 1$ **Twisted Gabidulin Codes**

J. Sheekey, A new family of linear maximum rank distance codes, 2016.

For $m = 1$ **Twisted Reed-Solomon Codes**

P. Beelen, S. Puchinger, and J. Rosenkilde, Twisted Reed-Solomon codes, 2017.

TZ-Type Construction

- $\mathbb{K} \subseteq \mathbb{E} \subseteq \mathbb{L}$ with $[\mathbb{L} : \mathbb{E}] = 2$,
- $\gamma \in \mathbb{L}^*$ such that $\mathbf{N}_{\mathbb{L}/\mathbb{K}}(\gamma) \notin \mathbb{K}^{(2)}$,
- $\{\lambda_1, \ldots, \lambda_\ell\} \subseteq \mathbb{K}^{(2)}$.

$$\mathcal{D}_{d,\sigma}(\gamma) := \left\{ P(X) \in {}^{\mathbb{L}[X;\sigma]}\!/_{(H_\lambda(X))} \mid \begin{array}{l} \deg(P(X)) \leq n-d+1, \\ a_0, \gamma a_{n-d+1} \in \mathbb{E} \end{array} \right\}.$$

Twisted Linearized Reed-Solomon Code of TZ-type

- $\dim_{\mathbb{K}}(\mathcal{D}_{d,\sigma}(\gamma)) = m(n-d+1)$,
- $\mathrm{wt}_{\mathrm{SR}}(P) \geq d$.

For $\ell = 1$ **Trombetti-Zhou Codes**

R. Trombetti and Y. Zhou, A new family of MRD codes in $\mathbb{F}_q^{2n\times 2n}$ with right and middle nuclei $\mathbb{F}_{q^n}$, 2016.

New MDS codes

For $m = 1$, we obtain

- $\gamma \in \mathbb{F}_{q^2} \setminus (\mathbb{F}_{q^2})^{(2)}$,
- $\{\lambda_1, \ldots, \lambda_n\} \subseteq (\mathbb{F}_{q^2})^{(2)}$.

$$\mathcal{D}_d(\gamma) := \left\{ P(X) \in \mathbb{F}_{q^2}[X] \mid \begin{array}{l} \deg(P(X)) \leq n-d+1, \\ a_0, \gamma a_{n-d+1} \in \mathbb{F}_q \end{array} \right\}$$

The **Twisted Linearized Reed-Solomon Code of TZ-type** is

$$\left\{ (P(\lambda_1), \ldots, P(\lambda_n)) \mid P(X) \in \mathcal{D}_d(\gamma) \right\} \subseteq \mathbb{F}_{q^2}^n.$$

It is a new $\mathbb{F}_q$-linear $(n, q^{2(n-d+1)}, d)$ **additive MDS code** over $\mathbb{F}_{q^2}$.

The construction works for every length

$$n \leq \frac{q^2+1}{2} \simeq \frac{|\mathbb{K}|}{2}.$$

The End

Thank you! **Danke!**

Grazie!