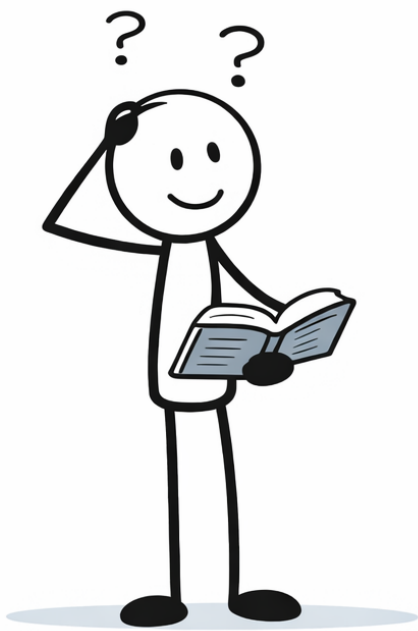
Toward a Unified Algebraic Framework for Reed-Solomon-Type Codes

Anna-Lena Horlemann

University of St.Gallen, Switzerland

OpeRa Workshop on Open Problems on Rank-Metric Codes
February 23rd 2026

Disclaimer



Please Note:

For clarity of presentation:

- Boundary cases are omitted.
- Some results are given in shortened form.

Thanks for understanding!

1. Reed-Solomon codes (Hamming metric)
2. Gabidulin codes (rank metric)
3. Linearized Reed-Solomon codes (sum-rank metric)
4. Skew Reed-Solomon codes (skew metric)
5. Connections between them
6. Open questions

Reed-Solomon codes (Hamming metric)

Hamming distance:

$$d_H(\mathbf{u}, \mathbf{v}) := |\{i \mid u_i \neq v_i\}|$$

Definition

Let $a_1, \ldots, a_n \in \mathbb{F}_q$ be distinct. Then

$$\mathrm{RS}[(a_1, \ldots, a_n); k, n]_q := \{(f(a_1), \ldots, f(a_n)) \mid f(x) \in \mathbb{F}_q[x], \deg(f) < k\}$$

is called a *Reed-Solomon code*.

RS-codes have minimum Hamming distance $n - k + 1$ and are MDS.

GRS and dual codes

- (Linear) isometries $=$ $\mathbb{F}_q$-monomial matrices
- A **generalized RS-code** is an RS-code with column multipliers $\mathbf{w} \in \mathbb{F}_q^n$.

GRS and dual codes

- (Linear) isometries $=$ $\mathbb{F}_q$-monomial matrices
- A **generalized RS-code** is an RS-code with column multipliers $\mathbf{w} \in \mathbb{F}_q^n$.

Theorem

1. *The dual of* $\mathrm{RS}[\mathbf{a}; k, n]_q$ *is* $\mathrm{GRS}[\mathbf{a}, \mathbf{w}; n-k, n]_q$ *with*

$$w_i := \Big(\prod_{i \neq j} (a_i - a_j)\Big)^{-1}.$$

2. *The dual of* $\mathrm{GRS}[\mathbf{a}, \mathbf{v}; k, n]_q$ *is* $\mathrm{GRS}[\mathbf{a}, \mathbf{w}; n-k, n]_q$ *with*

$$w_i := \Big(v_i \prod_{i \neq j} (a_i - a_j)\Big)^{-1}.$$

The Schur product $\star$

Evaluation is multiplicative (ring homomorphism):

$$[v \cdot f(a)][w \cdot g(a)] = vw(fg)(a)$$

Theorem

$$\mathrm{GRS}[\mathbf{a}, \mathbf{v}; k_1, n]_q \star \mathrm{GRS}[\mathbf{a}, \mathbf{w}; k_2, n]_q = \mathrm{GRS}[\mathbf{a}, \mathbf{v} \star \mathbf{w}; k_1 + k_2 - 1, n]_q$$

1. Reed-Solomon codes (Hamming metric)
2. Gabidulin codes (rank metric)
3. Linearized Reed-Solomon codes (sum-rank metric)
4. Skew Reed-Solomon codes (skew metric)
5. Connections between them
6. Open questions

Gabidulin codes (rank metric)

Rank distance:

$$d_R(\mathbf{u}, \mathbf{v}) := \mathrm{rk}_q(\mathbf{u} - \mathbf{v})$$

Linearized polynomial ring:

$$\mathcal{L}_{q^m}[x] := \left\{ \sum_{i=0}^{\delta-1} f_i x^{q^i} \mid f_i \in \mathbb{F}_{q^m} \right\}, \quad f \circ g(x) := f(g(x))$$

Definition

Let $a_1, \ldots, a_n \in \mathbb{F}_{q^m}$ be $\mathbb{F}_q$-linearly independent. Then

$$\mathrm{Gab}[\mathbf{a}; k, n]_{q^m} := \{(f(a_1), \ldots, f(a_n)) \mid f(x) \in \mathcal{L}_{q^m}[x], \deg(f) < k\}$$

is called a *Gabidulin code*.

Gabidulin codes have minimum rank distance $n - k + 1$ and are MRD.

Generalized Gabidulin and dual codes

- (Linear) isometries $= \mathrm{GL}_n(\mathbb{F}_q)$
- Gabidulin codes are closed under linear isometries

Generalized Gabidulin and dual codes

- (Linear) isometries $= \mathrm{GL}_n(\mathbb{F}_q)$
- Gabidulin codes are closed under linear isometries

Theorem

The dual of $\mathrm{Gab}[\mathbf{a}; k, n]_{q^m}$ *is* $\mathrm{Gab}[\mathbf{b}; n-k, n]_{q^m}$, *where* $\mathbf{b}$ *is trace-dual to* $\mathbf{a}$.

Generalized Gabidulin and dual codes

- (Linear) isometries $= \mathrm{GL}_n(\mathbb{F}_q)$
- Gabidulin codes are closed under linear isometries

Theorem

The dual of $\mathrm{Gab}[\mathbf{a}; k, n]_{q^m}$ *is* $\mathrm{Gab}[\mathbf{b}; n-k, n]_{q^m}$*, where* $\mathbf{b}$ *is trace-dual to* $\mathbf{a}$*.*

- A **generalized Gabidulin-code** is a Gabidulin code with q^s-linearized polynomials.
- Its dual is again a generalized Gabidulin code.

The Frobenius intersection/sum

Twisted ring homomorphism:

$$f(a)^q = f^{(q)}(a^q)$$

Theorem

$$\mathrm{Gab}[\mathbf{a}; k_1, n]_{q^m} \cap \mathrm{Gab}[\mathbf{a}; k_2, n]_{q^m}^{(q)} = \mathrm{Gab}[\mathbf{a}^{(q)}; \min(k_1 - 1, k_2), n]_{q^m}$$

$$\Longleftrightarrow$$

$$\mathrm{Gab}[\mathbf{a}; k_1, n]_{q^m} + \mathrm{Gab}[\mathbf{a}; k_2, n]_{q^m}^{(q)} = \mathrm{Gab}[\mathbf{a}; \max(k_2 + 1, k_1), n]_{q^m}$$

1. Reed-Solomon codes (Hamming metric)
2. Gabidulin codes (rank metric)
3. Linearized Reed-Solomon codes (sum-rank metric)
4. Skew Reed-Solomon codes (skew metric)
5. Connections between them
6. Open questions

Linearized Reed-Solomon codes (sum-rank metric)

Sum-rank distance: $d_{SR}(\mathbf{u}, \mathbf{v}) := \sum_{i=1}^{\eta} \mathrm{rk}_q(\mathbf{u}_i - \mathbf{v}_i)$

Skew polynomial ring: $\mathbb{F}_{q^m}[x;\theta] := \left\{ \sum_{i=0}^{\delta-1} f_i x^i \mid f_i \in \mathbb{F}_{q^m} \right\}$

$$x f_i = \theta(f_i) x, \quad f(b)_a := \sum_{i=0}^{\delta-1} f_i \theta^i(b) a^{\frac{q^{is}-1}{q^s-1}}$$

Definition

Let $\theta = x^{q^s}$ be a field automorphism and $a_1, \ldots, a_\eta \in \mathbb{F}_{q^m}$ be from pairwise distinct θ-conjugacy classes. Moreover, let $\mathbf{b} = (\mathbf{b}_1, \ldots, \mathbf{b}_\eta)$ have full sum-rank weight. Then

$$\mathrm{LRS}[\mathbf{a}, \mathbf{b}; k, n]^{\theta}_{q^m} := \{(f(\mathbf{b}_1)_{a_1}, \ldots, f(\mathbf{b}_n)_{a_\eta}) \mid f \in \mathbb{F}_{q^m}[x;\theta], \deg(f) < k\}$$

is called a *linearized Reed-Solomon code*.

LRS-codes have minimum sum-rank distance $\eta n - k + 1$ and are MSRD.

GLRS and dual codes

- (Linear) isometries $=$ $\mathbb{F}_{q^m}$-block monomial matrices with $\mathrm{GL_n}(\mathbb{F}_q)$-blocks
- A **generalized LRS-code** is an LRS-code with block multipliers $\mathbf{w} \in \mathbb{F}_{q^m}^n$.

GLRS and dual codes

- (Linear) isometries = $\mathbb{F}_{q^m}$-block monomial matrices with $\mathrm{GL_n}(\mathbb{F}_q)$-blocks
- A **generalized LRS-code** is an LRS-code with block multipliers $\mathbf{w} \in \mathbb{F}_{q^m}^n$.

Theorem

1. *The dual of* $\mathrm{LRS}[\mathbf{a}, \mathbf{b}; k, n]_{q^m}^{\theta}$ *is a generalized linearized Goppa code.*
2. *If the trace-dual* $\mathbf{b}'$ *of* $\mathbf{b}$ *has full sum-rank weight, then the dual of* $\mathrm{LRS}[\mathbf{a}, \mathbf{b}; k, n]_{q^m}^{\theta}$ *is* $\mathrm{LRS}[\theta(\mathbf{a})^{-1}, \mathbf{b}'; n-k, n]_{q^m}^{\theta^{-1}}$.
3. *In general, the dual of* $\mathrm{GLRS}[\mathbf{a}, \mathbf{v}; k, n]_q$ *contains the respective GLRS-Code, but is not necessarily equal.*

1. Reed-Solomon codes (Hamming metric)
2. Gabidulin codes (rank metric)
3. Linearized Reed-Solomon codes (sum-rank metric)
4. Skew Reed-Solomon codes (skew metric)
5. Connections between them
6. Open questions

Skew Reed-Solomon codes (skew metric)

Skew distance:

$$d_S^{\theta,\alpha}(\mathbf{u},\mathbf{v}) := \deg(\mathrm{lclm}_{i=1,\dots,n}\{x-\theta(u_i-v_i)\alpha_i(u_i-v_i)^{-1} \mid v_i \neq 0\})$$

Skew polynomial ring: $\mathbb{F}_{q^m}[x;\theta] := \left\{\sum_{i=0}^{\delta-1} f_i x^i \mid f_i \in \mathbb{F}_{q^m}\right\}$

$$xf_i = \theta(f_i)x, \quad f[a] := \sum_{i=0}^{\delta-1} f_i b^{\frac{q^{is}-1}{q^s-1}}$$

Definition

Let $a_1,\dots,a_n \in \mathbb{F}_{q^m}$ be P_θ-linearly independent (i.e., full skew weight).

$$\mathrm{SRS}[\mathbf{a};k,n]_{q^m}^{\theta} := \{(f[a_1],\dots,f[a_n]) \mid f \in \mathbb{F}_{q^m}[x;\theta], \deg(f) < k\}$$

is called a *skew Reed-Solomon code*.

SRS-codes have minimum skew distance $n-k+1$ and are MSD.

Dual codes and ring homomorphisms

... analog to the linearized case ...

1. Reed-Solomon codes (Hamming metric)
2. Gabidulin codes (rank metric)
3. Linearized Reed-Solomon codes (sum-rank metric)
4. Skew Reed-Solomon codes (skew metric)
5. Connections between them
6. Open questions

From linearized to skew – and back

Theorem (From GLRS to GSRS codes)

$$\mathrm{GLRS}[\mathbf{a}, \mathbf{b}, \mathbf{w}; k, n]^{\theta}_{q^m} = \mathrm{GSRS}[\gamma_\theta(\mathbf{b}, \mathbf{a}), \mathbf{w} \star \mathbf{a}; k, n]^{\theta}_{q^m}$$

Theorem (From GSRS to GLRS codes)

Let $\mathbf{a}, \mathbf{b} \in \mathbb{F}_{q^m}^n$ *such that* $\pi(\alpha) = \gamma_\theta(\mathbf{b}, \mathbf{a})$. *Then,*

$$\mathrm{GSRS}[\pi(\alpha), \mathbf{w}; k, n]^{\theta}_{q^m} = \mathrm{GLRS}[\mathbf{a}, \mathbf{b}, \mathbf{w} \star \mathbf{b}^{-1}; k, n]^{\theta}_{q^m}.$$

GRS and Gabidulin codes as GSRS/GSRS codes

Theorem (GRS as GSRS/GLRS codes)

$$\mathrm{GRS}[\mathbf{b}, \mathbf{w}; k, n]_{q^m} = \mathrm{GSRS}[\mathbf{b}, \mathbf{w}; k, n]^{\mathrm{id}}_{q^m} = \mathrm{GLRS}[\mathbf{1}, \mathbf{b}, \mathbf{w}; k, n]^{\mathrm{id}}_{q^m}$$

Theorem (Gabidulin as GSRS/GLRS codes)

Let $\sigma(x) = x^q$ denote the Frobenius map. Then

$$\mathrm{Gab}[\mathbf{b}; k, n]_{q^m} = \mathrm{GSRS}[\mathbf{b}^{q-1}, \mathbf{b}; k, n]^{\sigma}_{q^m} = \mathrm{GLRS}[\mathbf{b}, (1), \mathbf{1}; k, n]^{\sigma}_{q^m}.$$

1. Reed-Solomon codes (Hamming metric)
2. Gabidulin codes (rank metric)
3. Linearized Reed-Solomon codes (sum-rank metric)
4. Skew Reed-Solomon codes (skew metric)
5. Connections between them
6. Open questions

Open questions

- What about the duals of GLRS/GSRS codes?
  - Is there another type of duality, s.t. dual of GLRS is always GLRS?
  - Are there other parameters under which the dual of GLRS is GLRS?
  - If not, what is special about the cases where duality does not hold?

Open questions

- What about the duals of GLRS/GSRS codes?
  - Is there another type of duality, s.t. dual of GLRS is always GLRS?
  - Are there other parameters under which the dual of GLRS is GLRS?
  - If not, what is special about the cases where duality does not hold?
- Is there an operator on LRS codes that collapses to Schur product and Frobenius intersection in the special cases?

Open questions

- What about the duals of GLRS/GSRS codes?
  - Is there another type of duality, s.t. dual of GLRS is always GLRS?
  - Are there other parameters under which the dual of GLRS is GLRS?
  - If not, what is special about the cases where duality does not hold?
- Is there an operator on LRS codes that collapses to Schur product and Frobenius intersection in the special cases?
- Can we use these results for a characterization and classification of GSRS/GLRS codes?

Open questions

- What about the duals of GLRS/GSRS codes?
  - Is there another type of duality, s.t. dual of GLRS is always GLRS?
  - Are there other parameters under which the dual of GLRS is GLRS?
  - If not, what is special about the cases where duality does not hold?
- Is there an operator on LRS codes that collapses to Schur product and Frobenius intersection in the special cases?
- Can we use these results for a characterization and classification of GSRS/GLRS codes?
- What is the impact on cryptographic applications?