Covering Properties of Sum-Rank-Metric Codes

Cornelia Ott[1], Hedongliang Liu[2], Antonia Wachter-Zeh[2]

[1]Ulm University

[2]Technical University of Munich

Annual Allerton Conference on Communication, Control, and Computing 2022

September 30, 2022

Preliminaries of the sum-rank metric

Codes in Sum-Rank-Metric

- $\mathbb{F}_{q^m}$ Extension Field of $\mathbb{F}_q$
- Codelength $n = \eta \cdot \ell$ splitted into ℓ blocks, each of size η
- Linear Code $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ subspace of dimension k

$$\boldsymbol{c} = [\underbrace{\boldsymbol{c}_1}_{\in \mathbb{F}_{q^m}^{\eta}} \mid \boldsymbol{c}_2 \mid \dots \mid \boldsymbol{c}_\ell] \in \mathbb{F}_{q^m}^n$$

$$\boldsymbol{C} = [\underbrace{\boldsymbol{C}_1}_{\in \mathbb{F}_q^{m \times \eta}} \mid \boldsymbol{C}_2 \mid \dots \mid \boldsymbol{C}_\ell] \in \mathbb{F}_q^{m \times n}$$

ℓ-sum-rank weight/distance:

$$\mathrm{wt}_{SR,\ell}(\boldsymbol{c}) := \sum_{i=1}^{\ell} \mathrm{rk}_{\mathbb{F}_q}(\boldsymbol{C}_i) \leq \ell \cdot \underbrace{\mu}_{:=\min\{m,\eta\}}$$

$$\mathrm{d}_{SR,\ell}(\boldsymbol{c}, \boldsymbol{c}') := \mathrm{wt}_{SR,\ell}(\boldsymbol{c} - \boldsymbol{c}')$$

Preliminaries of the sum-rank metric

Spheres and Balls in Sum-Rank-Metric

Let $\tau \in \mathbb{Z}_{\geq 0}$ with $0 \leq \tau \leq \ell \cdot \mu$ and $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$. The sum-rank-metric sphere with radius τ and center $\boldsymbol{x}$ is defined as

$$\mathcal{S}_\ell(\boldsymbol{x}, \tau) := \{\boldsymbol{y} \in \mathbb{F}_{q^m}^n \mid \mathrm{d}_{SR,\ell}(\boldsymbol{x}, \boldsymbol{y}) = \tau\}.$$

Analogously, we define the ball of sum-rank-radius τ with center $\boldsymbol{x}$ by

$$\mathcal{B}_\ell(\boldsymbol{x}, \tau) := \bigcup_{i=0}^{\tau} \mathcal{S}_\ell(\boldsymbol{x}, i).$$

We also define the following cardinalities:

$$\mathrm{Vol}_{\mathcal{S}_\ell}(\tau) := |\{\boldsymbol{y} \in \mathbb{F}_{q^m}^n \mid \mathrm{wt}_{SR,\ell}(\boldsymbol{y}) = \tau\}|,$$
$$\mathrm{Vol}_{\mathcal{B}_\ell}(\tau) := \sum_{i=0}^{\tau} \mathrm{Vol}_{\mathcal{S}_\ell}(i).$$

Preliminaries of the sum-rank metric

Spheres and Balls in Sum-Rank-Metric

Let $\tau \in \mathbb{Z}_{\geq 0}$ with $0 \leq \tau \leq \ell \cdot \mu$ and $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$. The sum-rank-metric sphere with radius τ and center $\boldsymbol{x}$ is defined as

$$\mathcal{S}_\ell(\boldsymbol{x}, \tau) := \{\boldsymbol{y} \in \mathbb{F}_{q^m}^n \mid \mathrm{d}_{SR,\ell}(\boldsymbol{x}, \boldsymbol{y}) = \tau\}.$$

Analogously, we define the ball of sum-rank-radius τ with center $\boldsymbol{x}$ by

$$\mathcal{B}_\ell(\boldsymbol{x}, \tau) := \bigcup_{i=0}^{\tau} \mathcal{S}_\ell(\boldsymbol{x}, i).$$

We also define the following cardinalities:

$$\mathrm{Vol}_{\mathcal{S}_\ell}(\tau) := |\{\boldsymbol{y} \in \mathbb{F}_{q^m}^n \mid \mathrm{wt}_{SR,\ell}(\boldsymbol{y}) = \tau\}|,$$

$$\mathrm{Vol}_{\mathcal{B}_\ell}(\tau) := \sum_{i=0}^{\tau} \mathrm{Vol}_{\mathcal{S}_\ell}(i).$$

Preliminaries of the sum-rank metric

Intersection of Balls in Sum-Rank-Metric

We can define the volume of the intersection of two equal sized balls $|\mathcal{B}_\ell(\boldsymbol{x}_1, \tau) \cap \mathcal{B}_\ell(\boldsymbol{x}_2, \tau)|$ independently of their centers but only dependent on their radii τ and the distance $\delta := \mathrm{d}_{SR,\ell}(\boldsymbol{x}_1, \boldsymbol{x}_2)$ between their respective centers as follows:

$$\mathrm{Vol}_{\mathcal{I}_\ell}(\tau, \delta) := |\{\boldsymbol{y} \in \mathbb{F}_{q^m}^n | \mathrm{wt}_{SR,\ell}(\boldsymbol{y}) \leq \tau \wedge \mathrm{d}_{SR,\ell}(\boldsymbol{y}, \boldsymbol{d}) \leq \tau\}|,$$

where $\boldsymbol{d} \in \mathbb{F}_{q^m}^n$ arbitrary but fix with $\mathrm{wt}_{SR,\ell}(\mathrm{d}) = \delta$. Obviously if $\delta > 2\tau$, then $\mathrm{Vol}_{\mathcal{I}_\ell}(\tau, \delta) = 0$.

Preliminaries of the sum-rank metric

Relation between the different metrics

For $x \in \mathbb{F}_{q^m}$ it holds that $\mathrm{wt}_{SR,\ell}(x) \leq \mathrm{wt}_{SR,n}(x)$.
Proof: $\boldsymbol{x} = [\boldsymbol{x}_1|\ldots|\boldsymbol{x}_\ell] \in \mathbb{F}_{q^m}^n$ with
$\mathrm{wt}_{SR,n}(\boldsymbol{x}) = n - t = \eta - t_1 + \ldots + \eta - t_\ell$ where $\sum_{i=1}^{\ell} t_i = t$ and each $\boldsymbol{x}_i$ has t_i zero entries. For the sum-rank weight one gets $\mathrm{wt}_{SR,\ell}(\boldsymbol{x}) = \sum_{i=1}^{\ell} \mathrm{rk}_q(\boldsymbol{x}_i) \leq \sum_{i=1}^{\ell} \min\{m, \eta - t_i\} \leq \sum_{i=1}^{\ell}(\eta - t_i) = n - t = \mathrm{wt}_{SR,n}(\boldsymbol{x})$.

For $x \in \mathbb{F}_{q^m}$ it holds that $\mathrm{wt}_{SR,1}(x) \leq \mathrm{wt}_{SR,\ell}(x)$.
Proof: Assume w.l.o.g. $n \leq m$ and let
$\mathrm{wt}_{SR,\ell}(\boldsymbol{x}) = t = t_1 + \ldots + t_\ell$ (i.e., each $\boldsymbol{x}_i$ has t_i $\mathbb{F}_q$-linearly independent columns for $i \in \{1, \ldots \ell\}$) $\Rightarrow \boldsymbol{x}$ has at most t $\mathbb{F}_q$-linearly independent columns in the union of all blocks, which corresponds to the rank weight of $\boldsymbol{x}$.

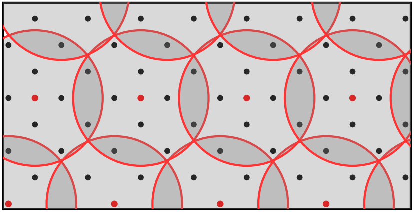
Covering Properties

Covering radius

Definition

Let $\mathcal{C}$ be a linear $[n, k, d]$ sum-rank metric code over $\mathbb{F}_{q^m}$. The covering radius of $\mathcal{C}$ is the smallest integer $\rho_{SR,\ell}$ such that every vector $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ has at most sum-rank distance $\rho_{SR,\ell}$ to some codeword $\boldsymbol{c} \in \mathcal{C}$ i.e., $\rho_{SR,\ell} = \max_{\boldsymbol{x} \in \mathbb{F}_{q^m}^n} \{\mathrm{d}_{SR,\ell}(\boldsymbol{x}, \mathcal{C})\}$.

$\mathbb{F}_{q^m}^n$



- $\in \mathbb{F}_{q^m}^n$
- $\in \mathcal{C}$

Covering Properties

Covering Problem for the sum-rank metric

For a given vectorspace $\mathbb{F}_{q^m}^n$ and a given integer ρ we denote the minimum cardinality of a code $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ with sum-rank covering radius ρ by $\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho)$. We now formulate the sphere covering problem for the sum-rank metric.

Problem

Find the minimum number of sum-rank balls $\mathcal{B}_\ell(\boldsymbol{x}, \rho)$ of radius ρ (with $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$) that cover the space $\mathbb{F}_{q^m}^n$ entirely. This problem is equivalent to determining the minimum cardinality $\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho)$ of a code $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ with sum-rank covering radius ρ.

Covering Properties

Covering Problem: Extreme Cases

There are two extreme cases for the covering radius:

(i) $\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, 0) = q^{mn}$, since from $\rho_{SR,\ell} = \max_{x \in \mathbb{F}_{q^m}^n} \{\mathrm{d}_{SR,\ell}(\boldsymbol{x}, \mathcal{C})\} = 0$ it follows that $\mathrm{d}_{SR,\ell}(\boldsymbol{x}, \mathcal{C}) = 0, \forall \boldsymbol{x} \in \mathbb{F}_{q^m}^n$ and therefore $\boldsymbol{x} \in \mathcal{C}$, i.e., $\mathcal{C} = \mathbb{F}_{q^m}^n$.

(ii) $\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \mu\ell) = 1$. Consider $\rho_{SR,\ell} = \max_{x \in \mathbb{F}_{q^m}^n} \{\mathrm{d}_{SR,\ell}(\boldsymbol{x}, \mathcal{C})\} = \mu \cdot \ell$ which means that there exists an $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ such that $\mathrm{d}_{SR,\ell}(\boldsymbol{x}, \mathcal{C}) = \mu \cdot \ell$. This is already fulfilled by choosing $\mathcal{C} = \{(0, \ldots, 0)\}$.

Covering Properties

Covering radii in different metrics

Lemma

Let $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ then it holds for its corresponding covering radii $\rho_{SR,1}$, $\rho_{SR,\ell}$ and $\rho_{SR,n}$ in the rank, the sum-rank and the Hamming metric that

$$\rho_{SR,1} \leq \rho_{SR,\ell} \leq \rho_{SR,n}.$$

Proof.

Since $\mathrm{wt}_{SR,1}(\boldsymbol{x}) \leq \mathrm{wt}_{SR,\ell}(\boldsymbol{x}) \leq \mathrm{wt}_{SR,n}(\boldsymbol{x})$ for a fix $\boldsymbol{x} \in \mathbb{F}_{q^m}$ it follows that $\mathrm{d}_{SR,1}(\boldsymbol{x}, \mathcal{C}) \leq \mathrm{d}_{SR,\ell}(\boldsymbol{x}, \mathcal{C}) \leq \mathrm{d}_{SR,n}(\boldsymbol{x}, \mathcal{C})$ and hence $\max_{\boldsymbol{x} \in \mathbb{F}_{q^m}^n} \{\mathrm{d}_{SR,1}(\boldsymbol{x}, \mathcal{C})\} \leq \max_{\boldsymbol{x} \in \mathbb{F}_{q^m}^n} \{\mathrm{d}_{SR,\ell}(\boldsymbol{x}, \mathcal{C})\} \leq \max_{\boldsymbol{x} \in \mathbb{F}_{q^m}^n} \{\mathrm{d}_{SR,n}(\boldsymbol{x}, \mathcal{C})\}$. □

Covering Properties

Comparison of the different metrics

Theorem

For $0 < \rho < \mu \cdot \ell$*, it holds*
$\mathcal{K}_{SR,1}(\mathbb{F}_{q^m}^n, \rho) \leq \mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho) \leq \mathcal{K}_{SR,n}(\mathbb{F}_{q^m}^n, \rho)$.

Proof.

Let $\mathcal{A}_{SR,\ell} := \{\mathcal{C} \subset \mathbb{F}_{q^m}^n \,|\, \bigcup_{\boldsymbol{c}\in\mathcal{C}} \mathcal{B}_\ell(\boldsymbol{c}, \rho) \supset \mathbb{F}_{q^m}^n\}$ be the set of codes with sum-rank covering radius ρ. Since $\mathrm{wt}_{SR,1}(\boldsymbol{x}) \leq \mathrm{wt}_{SR,\ell}(\boldsymbol{x}) \leq \mathrm{wt}_{SR,n}(\boldsymbol{x})$ for a fix $\boldsymbol{x} \in \mathbb{F}_{q^m}$, one gets $\bigcup_{\boldsymbol{c}\in\mathcal{C}} \mathcal{B}_1(\boldsymbol{c}, \rho) \supset \bigcup_{\boldsymbol{c}\in\mathcal{C}} \mathcal{B}_\ell(\boldsymbol{c}, \rho) \supset \bigcup_{\boldsymbol{c}\in\mathcal{C}} \mathcal{B}_n(\boldsymbol{c}, \rho)$ and hence it follows that $\mathcal{A}_{SR,1} \supset \mathcal{A}_{SR,\ell} \supset \mathcal{A}_{SR,n}$. With $\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho) = \min_{\mathcal{C}\in\mathcal{A}_{SR,\ell}}\{|\mathcal{C}|\}$ the statement follows. □

Theorem (Sphere Covering Bound)

For the minimum cardinality of a code $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ with sum-rank covering radius $0 < \rho < \mu \cdot \ell$ the following inequality holds:

$$\frac{q^{mn}}{\mathrm{Vol}_{\mathcal{B}_\ell}(\rho)} \leq \mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho).$$

Proof.

If it is possible to cover the whole space $\mathbb{F}_{q^m}^n$ with balls of radius ρ without overlapping any two balls, then $\frac{q^{mn}}{\mathrm{Vol}_{\mathcal{B}_\ell}(\rho)} = \mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho)$. This is only possible for perfect sum-rank metric codes. If there are overlapping balls then $\frac{q^{mn}}{\mathrm{Vol}_{\mathcal{B}_\ell}(\rho)} < \mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho)$. □

Lower Bounds for the Sphere Covering Problem

Simplified Sphere Covering Bound

Theorem (Simplified Sphere Covering Bound)

For $0 < \rho < \mu \cdot \ell$ *the following inequality holds:*

$$\frac{q^{mn-\rho(m+\eta-\frac{\rho}{\ell})}}{\rho \cdot \binom{\ell+\rho-1}{\ell-1}\gamma_q^\ell} \leq \mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho)$$

Proof.

$$\mathrm{Vol}_{\mathcal{S}_\ell}(\rho) \leq \binom{\ell+\rho-1}{\ell-1}\gamma_q^\ell q^{\rho(m+\eta-\frac{\rho}{\ell})} \quad \text{[PRR22, Theorem 5].}$$

Since $\mathrm{Vol}_{\mathcal{B}_\ell}(\rho) = \sum_{\rho'=0}^{\rho} \mathrm{Vol}_{\mathcal{S}_\ell}(\rho') \leq \rho \mathrm{Vol}_{\mathcal{S}_\ell}(\rho)$ for $\rho > 1$, this gives an upper bound on $\mathrm{Vol}_{\mathcal{B}_\ell}(\rho)$. Plugging in this upper bound in the sphere covering Bound leads to the claim. □

Lower Bounds for the Sphere Covering Problem

Theorem

For the covering radius ρ fulfilling $0 < \rho < \mu \cdot \ell$ the minimum cardinality $\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n)$ of a code is greater than 3.

Theorem

Let $0 < \rho < \mu \cdot \ell$ and $0 < k \leq \lfloor \log_{q^m}(\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho)) \rfloor$ then

$$\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho) \geq \frac{1}{\mathrm{Vol}_{\mathcal{B}_\ell}(\rho) - \mathrm{Vol}_{\mathcal{I}_\ell}(\rho, \mu\ell - \frac{\mu}{\eta}k)}$$

$$\cdot \Big(q^{mn} - q^{km}\mathrm{Vol}_{\mathcal{I}_\ell}(\rho, \mu\ell - \frac{\mu}{\eta}k) + \mathrm{Vol}_{\mathcal{I}_\ell}(\rho, \mu\ell - \frac{\mu}{\eta}k + 1)$$

$$\cdot \sum_{k'=\max\{1, n-2\frac{\eta}{\mu}\rho+1\}}^{k} (q^{k'm} - q^{(k'-1)m}) \Big).$$

Upper Bounds for the Sphere Covering Problem

Theorem

For the minimum cardinality of a code $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ with sum-rank covering radius $0 < \rho < \mu \cdot \ell$ the following inequality holds:
$\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho) \leq q^{m(n-\rho)}$.

Proof.

Consider a systematic generator matrix $\boldsymbol{G} = (\boldsymbol{I}|\boldsymbol{A})$ of a code $\mathcal{C}$. For each vector $\boldsymbol{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n$ there exists a codeword $\boldsymbol{c} = (x_1, \ldots, x_k, c_{k+1}, \ldots, c_n) \in \mathcal{C}$ with $\mathrm{d}_{SR,\ell}(\boldsymbol{x}, \boldsymbol{c}) = \mathrm{wt}_{SR,\ell}(0, \ldots, 0, \tilde{c}_{k+1}, \ldots, \tilde{c}_n) \leq \mathrm{wt}_{SR,n}(0, \ldots, 0, \tilde{c}_{k+1}, \ldots, \tilde{c}_n) \leq n - k$. Therefore $\min_{c \in \mathcal{C}}\{\mathrm{d}_{SR,\ell}(\boldsymbol{x}, \boldsymbol{c})\} \leq n - k$ for each $\boldsymbol{x} \in \mathbb{F}_{q^m}^n$ and hence $\rho = \max_{\boldsymbol{x} \in \mathbb{F}_{q^m}^n}\{\mathrm{d}_{SR,\ell}(\boldsymbol{x}, \mathcal{C})\} \leq n - k$. This leads to the upper bound $\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho) \leq |\mathcal{C}| = q^{mk} \leq q^{m(n-\rho)}$. □

Upper Bounds for the Sphere Covering Problem

Theorem

Let $0 \leq \rho \leq \mu \cdot \ell$ *then*

$$\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho) \leq q^{(m-\lfloor \frac{\rho}{\ell} \rfloor)\cdot(n-\rho)}.$$

Theorem

Let m, n, ρ *be fixed positive integers, then for any* l *with* $0 \leq l \leq n$ *and for every pair* (n_i, ρ_i) *fulfilling the following three conditions*

(i) $0 < n_i \leq n$

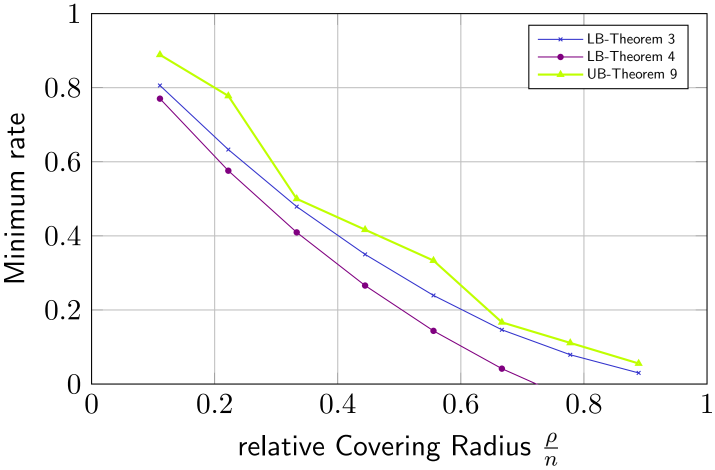
(ii) $0 \leq \rho_i \leq n_i$

(iii) $n_i + \rho_i \leq m$

for all $0 \leq i \leq l-1$ *with* $\sum_{i=0}^{l-1} n_i = n$ *and* $\sum_{i=0}^{l-1} \rho_i = \rho$ *it holds*

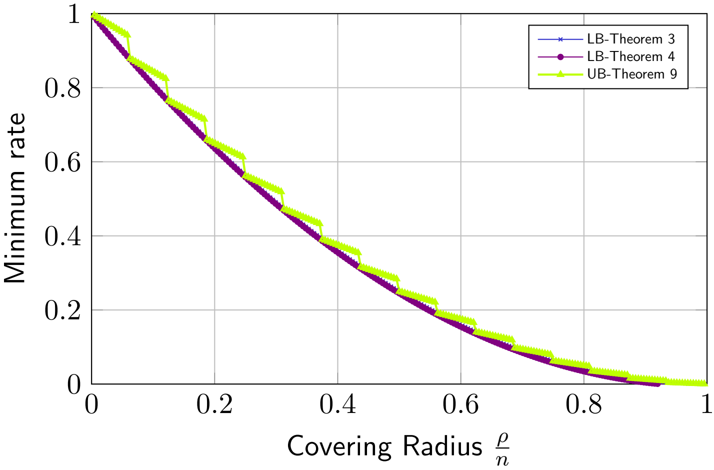
$$\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho) \leq \min_{l \in \{0,\ldots,n\}} q^{m(n-\rho)-\sum_{i=0}^{l-1}(\lfloor \frac{\rho_i}{\ell} \rfloor)\cdot(n_i-\rho_i)}$$

Numerical Comparison of the different Covering Bounds



Comparison of bounds on $\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho)$ for parameters $q = 4, m = 4, \eta = 3, \ell = 3, n = \eta\ell = 9$.

Numerical Comparison of the different Covering Bounds



Comparison of bounds on $\mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho)$ for parameters $q = 16, m = 16, \eta = 16, \ell = 14, n = \eta\ell = 224$.

Conclusion

- Relation between the different metrics
  - $\mathrm{wt}_{SR,1} \leq \mathrm{wt}_{SR,\ell} \leq \mathrm{wt}_{SR,n}$ (already known)
  - $\rho_{SR,1} \leq \rho_{SR,1} \leq \rho_{SR,n}$
  - $\mathcal{K}_{SR,1} \leq \mathcal{K}_{SR,\ell} \leq \mathcal{K}_{SR,n}$
- Upper and lower bounds on $\mathcal{K}_{SR,\ell}$
- Open Problem: Calculate $\mathrm{Vol}_{\mathcal{I}_\ell}$ exactly and efficiently and find an upper and a lower bound

References

[GY08] Maximilien Gadouleau and Zhiyuan Yan.
Packing and covering properties of rank metric codes.
IEEE Transactions on Information Theory, 54(9):3873–3883, 2008.

[GY09] Maximilien Gadouleau and Zhiyuan Yan.
Bounds on covering codes with the rank metric.
IEEE Communications Letters, 13(9):691–693, 2009.

[PRR22] Sven Puchinger, Julian Renner, and Johan Rosenkilde.
Generic decoding in the sum-rank metric.
IEEE Transactions on Information Theory, pages 1–1, 2022.