Covering Properties of Sum-Rank-Metric Codes

Cornelia Ott¹, Hedongliang Liu², Antonia Wachter-Zeh²

¹Ulm University
²Technical 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 $n = \eta \cdot \ell$ split into $\ell$ blocks, each of size $\eta$
- Linear Code $C \subset \mathbb{F}_q^{n \times m}$ subspace of dimension $k$

$$c = \left[ \begin{array}{c} c_1 \\ \vdots \\ c_\ell \end{array} \right] \in \mathbb{F}_{q^m}^\eta$$

$$C = \left[ \begin{array}{c} C_1 \\ \vdots \\ C_\ell \end{array} \right] \in \mathbb{F}_q^{m \times \eta}$$

$\ell$-sum-rank weight/distance:

$$w_{SR,\ell}(c) := \sum_{i=1}^{\ell} \text{rk}_{\mathbb{F}_q}(C_i) \leq \ell \cdot \mu$$

$$d_{SR,\ell}(c, c') := w_{SR,\ell}(c - c')$$

$\mu := \min\{m, \eta\}$
Let $\tau \in \mathbb{Z}_{\geq 0}$ with $0 \leq \tau \leq \ell \cdot \mu$ and $x \in \mathbb{F}_q^n$. The sum-rank-metric sphere with radius $\tau$ and center $x$ is defined as

$$S_\ell(x, \tau) := \{ y \in \mathbb{F}_q^n \mid d_{SR,\ell}(x, y) = \tau \}.$$ 

Analogously, we define the ball of sum-rank-radius $\tau$ with center $x$ by

$$B_\ell(x, \tau) := \bigcup_{i=0}^{\tau} S_\ell(x, i).$$

We also define the following cardinalities:

$$\text{Vol}_{S_\ell}(\tau) := \left| \{ y \in \mathbb{F}_q^n \mid \text{wt}_{SR,\ell}(y) = \tau \} \right|,$$

$$\text{Vol}_{B_\ell}(\tau) := \sum_{i=0}^{\tau} \text{Vol}_{S_\ell}(i).$$
Let $\tau \in \mathbb{Z}_{\geq 0}$ with $0 \leq \tau \leq \ell \cdot \mu$ and $x \in \mathbb{F}_q^n$. The sum-rank-metric sphere with radius $\tau$ and center $x$ is defined as

$$S_{\ell}(x, \tau) := \{ y \in \mathbb{F}_q^n \mid d_{SR,\ell}(x, y) = \tau \}.$$ 

Analogously, we define the ball of sum-rank-radius $\tau$ with center $x$ by

$$B_{\ell}(x, \tau) := \bigcup_{i=0}^{\tau} S_{\ell}(x, i).$$

We also define the following cardinalities:

$$\text{Vol}_{S_{\ell}}(\tau) := |\{ y \in \mathbb{F}_q^n \mid \text{wt}_{SR,\ell}(y) = \tau \}|,$$

$$\text{Vol}_{B_{\ell}}(\tau) := \sum_{i=0}^{\tau} \text{Vol}_{S_{\ell}}(i).$$
We can define the volume of the intersection of two equal sized balls $|B_\ell(x_1, \tau) \cap B_\ell(x_2, \tau)|$ independently of their centers but only dependent on their radii $\tau$ and the distance $\delta := d_{SR,\ell}(x_1, x_2)$ between their respective centers as follows:

$$\text{Vol}_{I_\ell}(\tau, \delta) := |\{y \in \mathbb{F}_{qm}^n | \text{wt}_{SR,\ell}(y) \leq \tau \land d_{SR,\ell}(y, d) \leq \tau\}|,$$

where $d \in \mathbb{F}_{qm}^n$ arbitrary but fix with $\text{wt}_{SR,\ell}(d) = \delta$. Obviously if $\delta > 2\tau$, then $\text{Vol}_{I_\ell}(\tau, \delta) = 0$. 
For \( x \in \mathbb{F}_{q^m} \) it holds that \( \text{wt}_{SR,\ell}(x) \leq \text{wt}_{SR,n}(x) \).

Proof: \( x = [x_1 | \ldots | x_\ell] \in \mathbb{F}_{q^m}^n \) with

\[
\text{wt}_{SR,n}(x) = n - t = \eta - t_1 + \ldots + \eta - t_\ell \quad \text{where} \quad \sum_{i=1}^\ell t_i = t \quad \text{and each} \quad x_i \quad \text{has} \quad t_i \quad \text{zero entries. For the sum-rank weight one gets}
\]

\[
\text{wt}_{SR,\ell}(x) = \sum_{i=1}^\ell \text{rk}_q(x_i) \leq \sum_{i=1}^\ell \min\{m, \eta - t_i\} \leq \sum_{i=1}^\ell (\eta - t_i) = n - t = \text{wt}_{SR,n}(x).
\]

For \( x \in \mathbb{F}_{q^m} \) it holds that \( \text{wt}_{SR,1}(x) \leq \text{wt}_{SR,\ell}(x). \)

Proof: Assume w.l.o.g. \( n \leq m \) and let

\[
\text{wt}_{SR,\ell}(x) = t = t_1 + \ldots + t_\ell \quad \text{(i.e., each} \quad x_i \quad \text{has} \quad t_i \quad \mathbb{F}_q\text{-linearly independent columns for} \ i \in \{1, \ldots, \ell\} \Rightarrow x \quad \text{has at most} \ t \quad \mathbb{F}_q\text{-linearly independent columns in the union of all blocks, which corresponds to the rank weight of} \ x.
\]
Covering Properties

Covering radius

**Definition**

Let $C$ be a linear $[n, k, d]$ sum-rank metric code over $\mathbb{F}_{q^m}$. The covering radius of $C$ is the smallest integer $\rho_{SR, \ell}$ such that every vector $x \in \mathbb{F}_{q^m}^n$ has at most sum-rank distance $\rho_{SR, \ell}$ to some codeword $c \in C$ i.e., $\rho_{SR, \ell} = \max_{x \in \mathbb{F}_{q^m}^n} \{ d_{SR, \ell}(x, C) \}$. 
For a given vectorspace $\mathbb{F}_{q^m}^n$ and a given integer $\rho$ we denote the minimum cardinality of a code $\mathcal{C} \subset \mathbb{F}_{q^m}^n$ with sum-rank covering radius $\rho$ 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 $\mathcal{B}_\ell(x, \rho)$ of radius $\rho$ (with $x \in \mathbb{F}_{q^m}^n$) 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 $\rho$. 
There are two extreme cases for the covering radius:

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

(ii) $\mathcal{K}_{SR,\ell}(\mathbb{F}_{qm}^n, \mu \ell) = 1$. Consider $\rho_{SR,\ell} = \max_{x \in \mathbb{F}_{qm}^n} \{d_{SR,\ell}(x, C)\} = \mu \cdot \ell$ which means that there exists an $x \in \mathbb{F}_{qm}^n$ such that $d_{SR,\ell}(x, C) = \mu \cdot \ell$. This is already fulfilled by choosing $C = \{(0, \ldots, 0)\}$.
Covering Properties
Covering radii in different metrics

**Lemma**

Let $C \subset \mathbb{F}_{q^m}^n$ 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 $\text{wt}_{SR,1}(x) \leq \text{wt}_{SR,\ell}(x) \leq \text{wt}_{SR,n}(x)$ for a fix $x \in \mathbb{F}_{q^m}$ it follows that $d_{SR,1}(x, C) \leq d_{SR,\ell}(x, C) \leq d_{SR,n}(x, C)$ and hence

$$\max_{x \in \mathbb{F}_{q^m}^n} \{d_{SR,1}(x, C)\} \leq \max_{x \in \mathbb{F}_{q^m}^n} \{d_{SR,\ell}(x, C)\} \leq \max_{x \in \mathbb{F}_{q^m}^n} \{d_{SR,n}(x, C)\}.$$
Covering Properties
Comparison of the different metrics

Theorem

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

Proof.
Let $\mathcal{A}_{SR,\ell} := \{ C \subseteq \mathbb{F}^n_{q^m} \mid \bigcup_{c \in C} \mathcal{B}_\ell(c, \rho) \supset \mathbb{F}^n_{q^m} \}$ be the set of codes with sum-rank covering radius $\rho$. Since
\[ \text{wt}_{SR,1}(\mathbf{x}) \leq \text{wt}_{SR,\ell}(\mathbf{x}) \leq \text{wt}_{SR,n}(\mathbf{x}) \]
for a fix $\mathbf{x} \in \mathbb{F}^n_{q^m}$, one gets
\[ \bigcup_{c \in C} \mathcal{B}_1(c, \rho) \supset \bigcup_{c \in C} \mathcal{B}_\ell(c, \rho) \supset \bigcup_{c \in C} \mathcal{B}_n(c, \rho) \]
and hence it follows that $\mathcal{A}_{SR,1} \supset \mathcal{A}_{SR,\ell} \supset \mathcal{A}_{SR,n}$. With
\[ \mathcal{K}_{SR,\ell}(\mathbb{F}^n_{q^m}, \rho) = \min_{C \in \mathcal{A}_{SR,\ell}} |C| \]
the statement follows.
Lower Bounds for the Sphere Covering Problem

Sphere Covering Bound

**Theorem (Sphere Covering Bound)**

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

\[
\frac{q^{mn}}{\text{Vol}_{B_\ell}(\rho)} \leq \mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho).
\]

**Proof.**

If it is possible to cover the whole space \( \mathbb{F}_{q^m}^n \) with balls of radius \( \rho \) without overlapping any two balls, then

\[
\frac{q^{mn}}{\text{Vol}_{B_\ell}(\rho)} = \mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho).
\]

This is only possible for perfect sum-rank metric codes. If there are overlapping balls then

\[
\frac{q^{mn}}{\text{Vol}_{B_\ell}(\rho)} < \mathcal{K}_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho).
\]
Theorem (Simplified Sphere Covering Bound)

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

$$q^{mn-\rho(m+\eta-\frac{\rho}{\ell})} \leq K_{SR,\ell}(\mathbb{F}_q^n, \rho)$$

Proof.

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

Since $\text{Vol}_{B_\ell}(\rho) = \sum_{\rho'}^\rho \text{Vol}_{S_\ell}(\rho') \leq \rho \text{Vol}_{S_\ell}(\rho)$ for $\rho > 1$, this gives an upper bound on $\text{Vol}_{B_\ell}(\rho)$. Plugging in this upper bound in the sphere covering Bound leads to the claim.
For the covering radius \( \rho \) fulfilling \( 0 < \rho < \mu \cdot \ell \) the minimum cardinality \( K_{SR,\ell}(\mathbb{F}_q^n) \) of a code is greater than 3.

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

\[
K_{SR,\ell}(\mathbb{F}_q^n, \rho) \geq \frac{1}{\text{Vol}_{B_\ell}(\rho) - \text{Vol}_{I_\ell}(\rho, \mu \ell - \frac{\mu}{\eta} k)} \cdot \left( q^{mn} - q^{km} \text{Vol}_{I_\ell}(\rho, \mu \ell - \frac{\mu}{\eta} k) + \text{Vol}_{I_\ell}(\rho, \mu \ell - \frac{\mu}{\eta} k + 1) \right) \cdot \sum_{k'=\max\{1,n\mu \rho + 1\}}^{k} \left( q^{k'm} - q^{(k'-1)m} \right).
\]
Theorem

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

\[
K_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho) \leq q^m(n-\rho).
\]

Proof.

Consider a systematic generator matrix \( G = (I|A) \) of a code \( C \). For each vector \( \mathbf{x} = (x_1, \ldots, x_n) \in \mathbb{F}_{q^m}^n \) there exists a codeword \( \mathbf{c} = (x_1, \ldots, x_k, c_{k+1}, \ldots, c_n) \in C \) with

\[
d_{SR,\ell}(\mathbf{x}, \mathbf{c}) = \text{wt}_{SR,\ell}(0, \ldots, 0, \tilde{c}_{k+1}, \ldots, \tilde{c}_n) \leq \text{wt}_{SR,n}(0, \ldots, 0, \tilde{c}_{k+1}, \ldots, \tilde{c}_n) \leq n - k.
\]

Therefore

\[
\min_{\mathbf{c} \in C} \{d_{SR,\ell}(\mathbf{x}, \mathbf{c})\} \leq n - k \text{ for each } \mathbf{x} \in \mathbb{F}_{q^m}^n \text{ and hence}
\]

\[
\rho = \max_{\mathbf{x} \in \mathbb{F}_{q^m}^n} \{d_{SR,\ell}(\mathbf{x}, C)\} \leq n - k.
\]

This leads to the upper bound

\[
K_{SR,\ell}(\mathbb{F}_{q^m}^n, \rho) \leq |C| = q^m k \leq q^m(n-\rho).
\]
Theorem

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

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

Theorem

Let $m$, $n$, $\rho$ be fixed positive integers, then for any $l$ with $0 \leq l \leq n$ and for every pair $(n_i, \rho_i)$ 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

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

Comparison of bounds on $K_{SR,\ell}(F_q^m, \rho)$ for parameters $q = 4$, $m = 4$, $\eta = 3$, $\ell = 3$, $n = \eta \ell = 9$. 
Comparison of bounds on $\mathcal{K}_{SR,\ell}(\mathbb{F}^n_{q^m}, \rho)$ for parameters $q = 16, m = 16, \eta = 16, \ell = 14, n = \eta \ell = 224$. 
Conclusion

- Relation between the different metrics
  - $w_{SR,1} \leq w_{SR,\ell} \leq w_{SR,n}$ (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 $\text{Vol}_{\mathcal{I}_\ell}$ 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.