ulm university universität ulm

Bounds and Genericity of Sum-Rank-Metric Codes

Cornelia Ott, Sven Puchinger, Martin Bossert

Redundancy 2021, Moscow

October 10, 2021

Outline

Motivation and Preliminaries

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

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

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

ℓ-sum-rank weight/distance:

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

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

Motivation and Preliminaries

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:

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

Bounds on Codes in Sum-Rank-Metric

Singleton like Bound [MPK19b, Corollary 4, 5][MPK19a, Theorem 5]]

Let $\mathcal{C}$ be a linear $[n, k, d]$ sum-rank metric code. Then it holds

$$k \leq \min\left\{n - d + 1, \frac{\eta}{m}\Big(\ell m - d + 1\Big)\right\}.$$

MSRD Codes

$\mathcal{C}$ is called *maximum sum-rank-distance* (MSRD), if the Singleton like Bound is fulfilled with equality.

Bounds on Codes in Sum-Rank-Metric

Sphere-Packing Bound

Sphere-Packing Bound[BGLR20, Theorem III.6]

For a linear $[n, k, d]$ sum-rank metric code $\mathcal{C}$, it holds that

$$q^{mk} \cdot \mathrm{Vol}_{\mathcal{B}_\ell}\left(\left\lfloor \frac{d-1}{2} \right\rfloor\right) \leq q^{mn}.$$

Both sides of the bounds can be computed in complexity $\tilde{\mathcal{O}}\left(\ell^2 d^3 + \ell d^4 (m+\eta)\log(q)\right)$ using the efficient algorithm for computing $\mathrm{Vol}_{\mathcal{S}_\ell}$ in [PRR20, Theorem 5 and Algorithm 1].

simplified Sphere-Packing Bound

For a linear $[n, k, d]$ sum-rank metric code $\mathcal{C}$, the parameters fulfill

$$q^{mk} \cdot q^{(m+\eta-\frac{1}{\ell}\lfloor\frac{d-1}{2}\rfloor)\lfloor\frac{d-1}{2}\rfloor-\frac{\ell}{4}} \cdot \gamma_q^{-\ell} \leq q^{mn}.$$

Bounds on Codes in Sum-Rank-Metric

Sphere-Packing Bound

asymptotic Sphere-Packing Bound

Let $\mathcal{C}$ be a linear $[n, k, d]$ sum-rank metric code and $\delta := \frac{d}{n}$ the relative minimum distance. Then the code rate $\mathcal{R} = \frac{k}{n}$ is upper bounded by

$$\mathcal{R} < \delta^2 \frac{\eta}{4m} - \delta\left(\frac{1}{2} + \frac{\eta}{m}\left(\frac{1}{2} + \frac{1}{n}\right)\right) + \frac{1}{n}\left(1 + \frac{\eta}{m} + \frac{\eta}{nm}\right) + \frac{1}{\eta m}\left(\frac{1}{4} + \log_q(\gamma_q)\right) + 1.$$

Let $\xi > 0$ be fixed.

- For $m = \eta\xi \to \infty$ we get $\mathcal{R} \sim \delta^2 \frac{1}{4\xi} - \frac{\delta}{2}\left(1 + \frac{1}{\xi}\right) + 1.$
- For $\ell \to \infty$ one get $\mathcal{R} \sim \delta^2 \frac{\eta}{4m} - \frac{\delta}{2}\left(1 + \frac{\eta}{m}\right) + \frac{1}{\eta m}\left(\frac{1}{4} + \log_q(\gamma_q)\right) + 1.$

Bounds on Codes in Sum-Rank-Metric

Gilbert–Varshamov Bound

Gilbert–Varshamov Bound[BGLR20, Theorem III.11]]

Let $\mathbb{F}_{q^m}$ be a finite field, $\ell, n, k, d \leq \mu\ell$ be positive integers that satisfy

$$q^{m(k-1)} \cdot \mathrm{Vol}_{\mathcal{B}_\ell}(d-1) < q^{mn}.$$

Then, there is a linear code of length n, dimension k, and minimum ℓ-sum-rank distance at least d.

simplified Gilbert–Varshamov Bound

Let $\mathbb{F}_{q^m}$ be a finite field, ℓ, n, k, d be positive integers with $2 < d \leq \mu\ell$ that satisfy

$$q^{m(k-1)} \cdot (d-1)\begin{pmatrix} \ell+d-2 \\ \ell-1 \end{pmatrix}\gamma_q^\ell q^{(d-1)(m+\eta-\frac{d-1}{\ell})} < q^{mn}.$$

Then, there is a linear code of length n, dimension k, and minimum ℓ-sum-rank distance at least d.

Bounds on Codes in Sum-Rank-Metric

Gilbert–Varshamov Bound

asymptotic Gilbert–Varshamov Bound

For a finite field $\mathbb{F}_{q^m}$ and positive integers $\ell, n, \mathcal{R}n, d$ with $\delta := \frac{d}{n}$ and $2 < d \leq \mu\ell$ satisfying

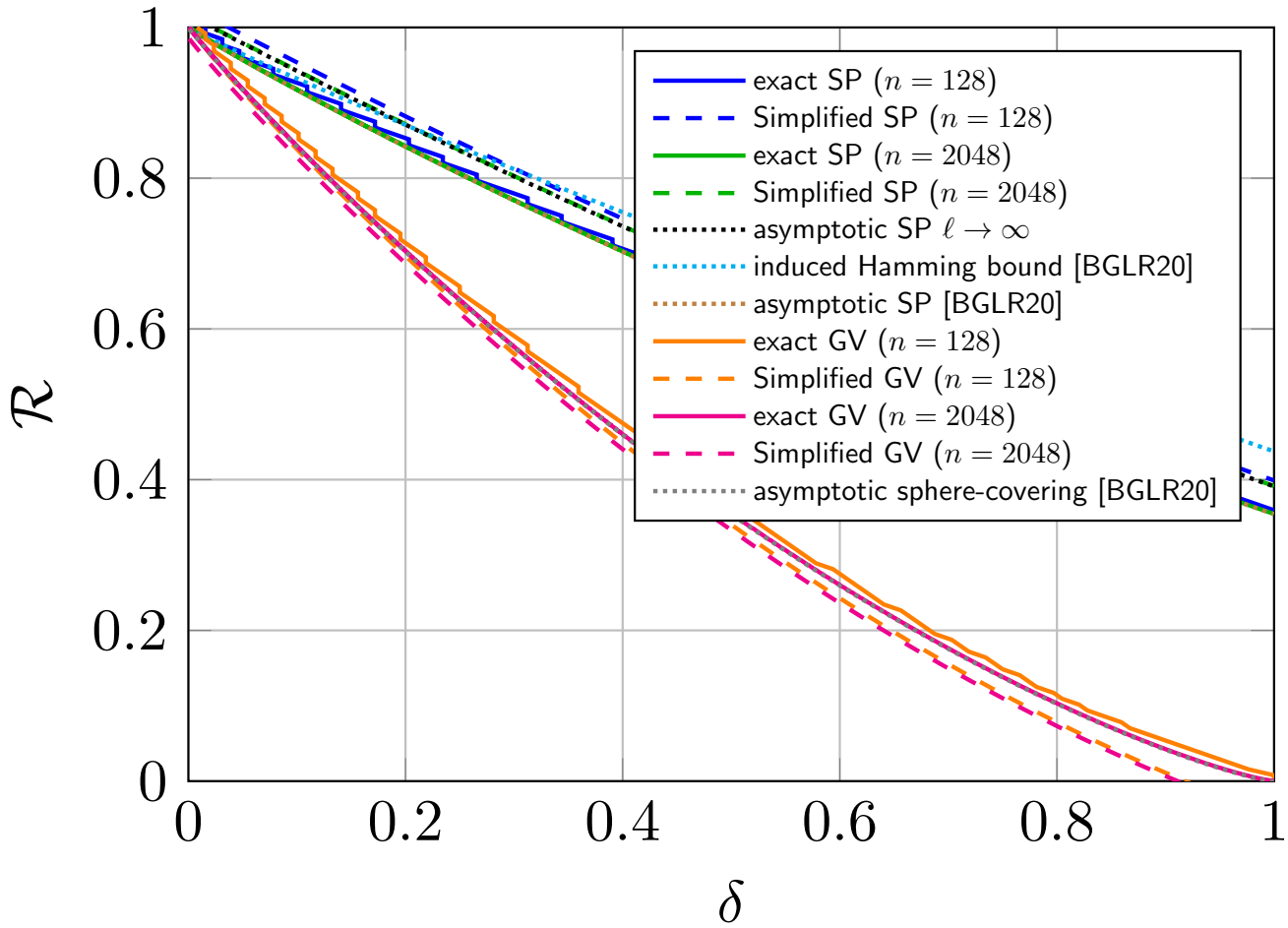
$$\begin{aligned}\mathcal{R} \leq & \delta^2 \frac{\eta}{m} - \delta\left(1 + \frac{\eta}{m} + \frac{2\eta}{nm}\right) + 1 + \frac{1}{n} + \frac{\eta}{nm} + \frac{\eta}{n^2 m} \\ & - \frac{\sum_{i=1}^{\delta n - 1} \log_q\left(1 + \frac{\ell - 1}{i}\right) + \log_q(\delta n - 1)}{mn} - \frac{\log_q(\gamma_q)}{\eta m}\end{aligned}$$

there exists a linear ℓ-sum-rank metric code of rate $\mathcal{R}$ and relative minimum sum-rank distance at least δ. Let ξ be a constant. For $m = \eta\xi \to \infty$ and $m \in \omega(\log_q(\ell))$ we have

$$\mathcal{R} \sim \delta^2 \frac{1}{\xi} - \delta\left(1 + \frac{1}{\xi}\right) + 1.$$

Bounds on Codes in Sum-Rank-Metric

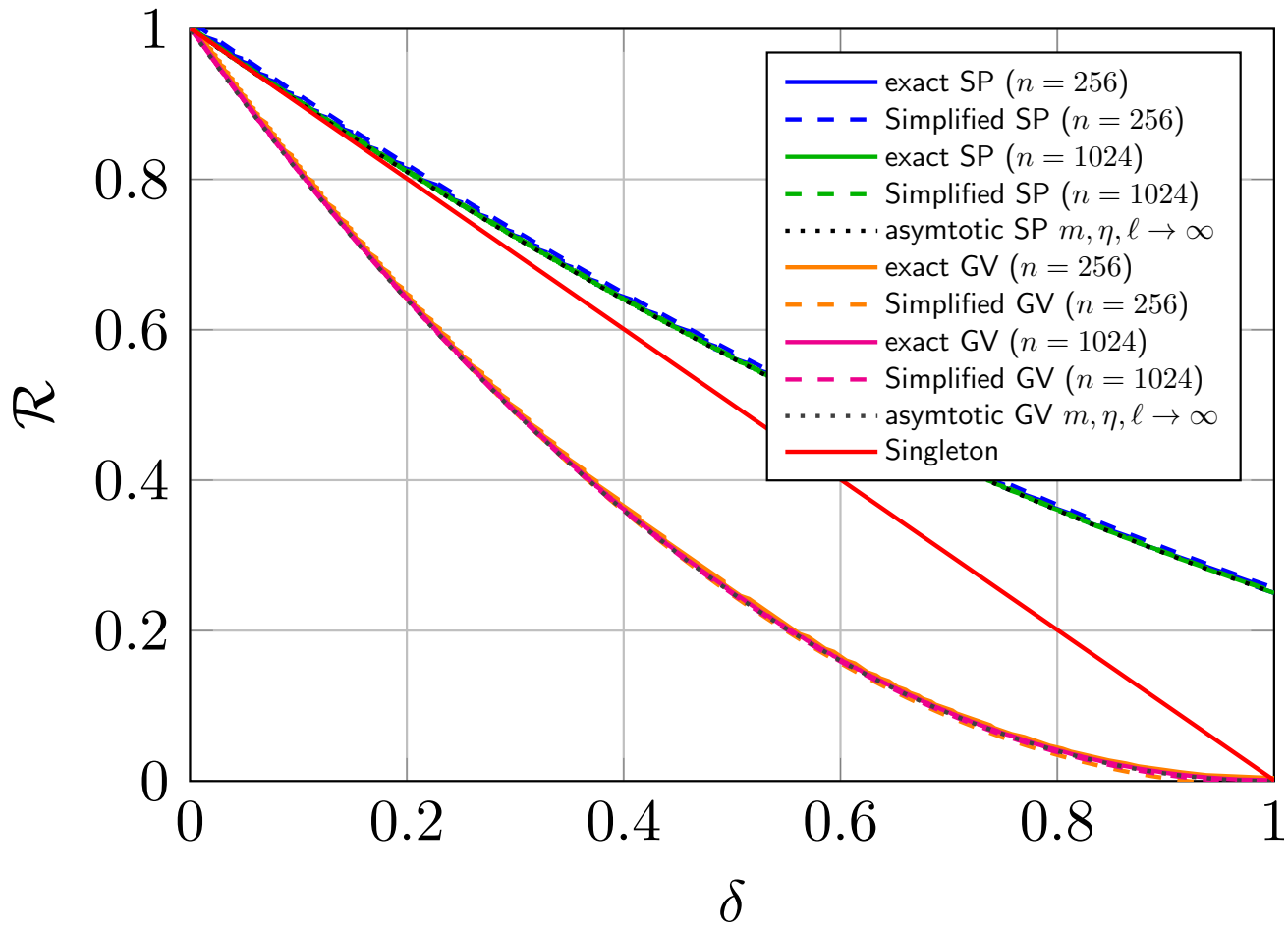
Numerical Comparisons: Bounded Blocksize



Comparison of different bounds for fixed value $q = 2$ $\eta = 8$ $m = 16$ for different values of n ($\ell = \frac{n}{\eta}$)

Simplified and Asymptotic Bounds

Numerical Comparisons: Growing Blocksize



Comparison of different bounds for fixed value of $q = 16$ and different values of n with $\eta = \ell = m$

Genericity Results

Random Linear Codes almost attain the GV bound with high probability

For q, m, n, d, choose $\epsilon \in \left(0, 1 - \log_q\left(\mathrm{Vol}_{\mathcal{B}_\ell}(d-1)^{\frac{1}{mn}}\right) - n^{-1}\right]$ and $k := n(1 - \log_q(\mathrm{Vol}_{\mathcal{B}_\ell}(d-1)^{\frac{1}{mn}}) - \epsilon)$. Let $\mathcal{C}$ be chosen uniformly at random from the set of linear codes length n and dimension k over $\mathbb{F}_{q^m}$. Then, $\mathcal{C}$ has minimum distance $\geq d$ with probability at least $1 - e^{-\Omega(mn)}$.

Genericity Results

Probability that Random codes are MSRD

Let p be the probabilty for a random linear ℓ-sum-rank distance Code of length n and dimension k to be MSRD. We derived the following bounds:

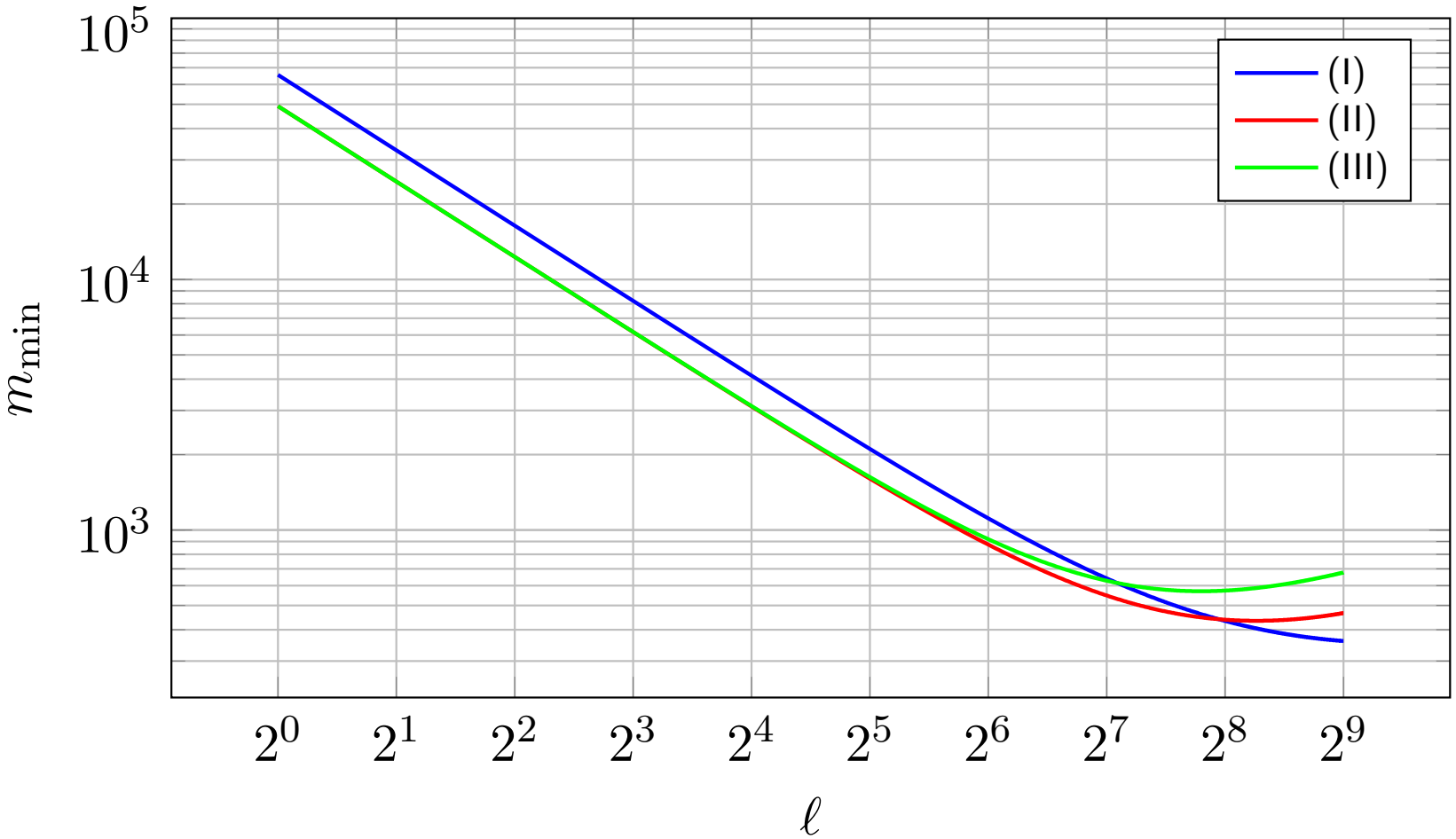
(I) $p \geq 1 - k\binom{k+\ell-1}{\ell-1} q^{\eta k - m}$
(c.f. [NHTRR18])

(II) $p \geq 1 - k\binom{k+\ell-1}{\ell-1} q^{k(\eta - \frac{k}{\ell}) - \frac{\ell}{4} - m} \cdot \gamma_q^{\ell}$
(c.f. [NHTRR18])

(III) $p \geq 1 - \frac{q^{mk}-1}{(q^m-1)(q^{mn}-1)} \left((n-k)\binom{\ell+n-k-1}{\ell-1} \gamma_q^{\ell} q^{(n-k)(m+\eta-\frac{n-k}{\ell})} - 1 \right)$
(c.f. [BR20])

Genericity Results

Probability that Random codes are MSRD



Comparison of the three bounds for $n = 2^9$, $k = 2^7$ and $q = 4$.

Conclusion

- simplified Sphere-packing and Gilbert–Varshamov bounds for codes in the sum-rank metric
- asymptotic bounds for sum-rank-metric codes whose block size grows in the code length
- comparison to exact bounds
- random linear sum-rank-metric codes achieve almost the sum-rank GV bound with high probability.
- bounds on the probability that a random linear code attains the sum-rank-metric Singleton bound

References

[BGLR20] Eimear Byrne, Heide Gluesing-Luerssen, and Alberto Ravagnani.
Fundamental properties of sum-rank metric codes, 2020.

[BR20] Eimear Byrne and Alberto Ravagnani.
Partition-balanced families of codes and asymptotic enumeration in coding theory.
Journal of Combinatorial Theory, Series A, 171:105169, 2020.

[MPK19a] Umberto Martínez-Peñas and Corollary 5.4]rank R Kschischang, F[20.
Reliable and secure multishot network coding using linearized reed-solomon codes.
IEEE Transactions on Information Theory, 2019.

[MPK19b] Umberto Martínez-Peñas and Frank R Kschischang.
Universal and dynamic locally repairable codes with maximal recoverability via sum-rank codes.
IEEE Transactions on Information Theory, 2019.

[NHTRR18] Alessandro Neri, Anna-Lena Horlemann-Trautmann, Tovohery Randrianarisoa, and Joachim Rosenthal.
On the genericity of maximum rank distance and gabidulin codes.
Designs, Codes and Cryptography, 86(2):341–363, 2018.

[OPB21] Cornelia Ott, Sven Puchinger, and Martin Bossert.
Bounds and Genericity of Sum-Rank-Metric Codes.
Extended version of this paper, arXiv:2102.02244, 2021.

[PRR20] Sven Puchinger, Julian Renner, and Johan Rosenkilde.
Generic Decoding in the Sum-Rank Metric.
arXiv preprint arXiv:2001.04812, 2020.