The geometry of covering codes in the sum-rank metric

Matteo Bonini

joint work with M. Borello and E. Byrne

WCC 2024

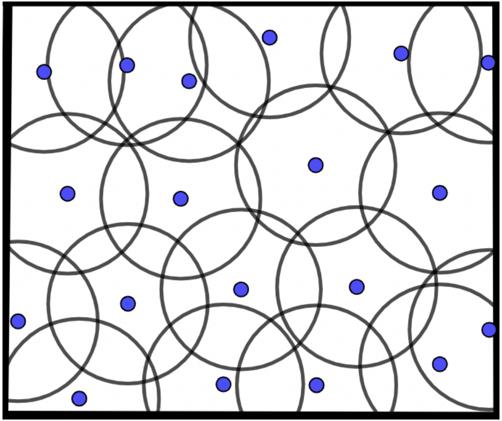
18^{th} **June 2024**

AALBORG UNIVERSITET

BREAKING NEW GROUND AALBORG UNIVERSITY

Preliminary notions

Covering Problem



Covering Radius

The **covering radius** of a code $\mathcal{C} \subseteq \mathcal{S}$ with respect to the metric d is the integer

$$\begin{aligned}\rho_d(\mathcal{C}) &:= \max\{\min\{d(x, c) : c \in \mathcal{C}\} : x \in \mathcal{S}\} \\ &= \min\{\rho : \cup_{x\in\mathcal{C}} \mathrm{B}(x, \rho) = \mathcal{S}\}\end{aligned}$$

The distances we will consider in this talk are

- Hamming metric d_{H}.
- Rank metric d_{rk}.
- Sum-rank metric d_{srk}.

Hamming and rank metrics

The **Hamming distance** is defined

$$\begin{aligned} d_{\mathrm{H}} : \mathbb{F}_q^n \times \mathbb{F}_q^n &\longrightarrow \mathbb{N} \\ (x, y) &\mapsto \mathrm{w}_{\mathrm{H}}(x - y) = |\{i : i \in \{1, \ldots, n\} \mid x_i \neq y_i\}| \end{aligned}$$

The **rank distance** is defined

$$\begin{aligned} d_{\mathrm{rk}} : \mathbb{F}_{q^m}^n \times \mathbb{F}_{q^m}^n &\longrightarrow \mathbb{N} \\ (\mathbf{x}, \mathbf{y}) &\mapsto \mathrm{w}_{\mathrm{rk}}(\mathbf{x} - \mathbf{y}) = \mathrm{rk}(\mathbf{Z}) \end{aligned}$$

where $\mathbf{Z} \in \mathbb{F}_q^{m \times n}$ is the matrix obtained representing the entries of $\mathbf{z} = \mathbf{x} - \mathbf{y} \in \mathbb{F}_{q^m}^n$ respect to a fixed basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

AALBORG UNIVERSITET

Sum-rank metric

Let t be a positive integer and $\mathbf{n} = (n_1, \ldots, n_t), \mathbf{m} = (m_1, \ldots, m_t) \in \mathbb{N}^t$ be ordered tuples with $n_1 \leq n_2 \leq \cdots \leq n_t$ and $m_1 \leq m_2, \leq \cdots \leq m_t$.

Let $X := (X_1, \ldots, X_t), Y = (Y_1, \ldots, Y_t) \in \mathrm{Mat}(\mathbf{n}, \mathbf{m}, \mathbb{F}_q)$.

The **sum-rank distance** is defined

$$d_{\mathrm{srk}} : \mathrm{Mat}_{\mathbf{n}\times\mathbf{m}}(\mathbb{F}_q) \times \mathrm{Mat}_{\mathbf{n}\times\mathbf{m}}(\mathbb{F}_q) \longrightarrow \mathbb{N}$$
$$(X, Y) \mapsto \mathrm{w}_{\mathrm{srk}}(X - Y) = \sum_{i=1}^{t} \mathrm{rk}(X_i - Y_i)$$

Saturating sets

AALBORG UNIVERSITET

Definition

A set $\mathcal{S} \subseteq \mathrm{PG}(k-1, q^m)$ is called ρ**-saturating** if for any point $Q \in \mathrm{PG}(k-1, q^m)$ there exist $\rho + 1$ points $P_1, \ldots, P_{\rho+1} \in \mathcal{S}$ such that $Q \in \langle P_1, \ldots, P_{\rho+1} \rangle_{\mathbb{F}_{q^m}}$ and ρ is the smallest value with this property.

$(\rho - 1)$-saturating sets of size n $\longleftrightarrow$ Duals of $[n, k]_{q^m}$ codes with Hamming covering radius ρ

Systems & Linear Sets

Definition

An $[n,k]_{q^m/q}$ **system** is an n-dimensional $\mathbb{F}_q$-space $\mathcal{U} \subseteq \mathbb{F}_{q^m}^k$ such that $\langle \mathcal{U} \rangle_{\mathbb{F}_{q^m}} = \mathbb{F}_{q^m}^k$. A **generator matrix** for $\mathcal{U}$ is a $k \times n$ matrix over $\mathbb{F}_{q^m}$ whose columns form an $\mathbb{F}_q$-basis for $\mathcal{U}$.

Definition

Let $\mathcal{U}$ be an $[n,k]_{q^m/q}$ system. The $\mathbb{F}_q$**-linear set** in of rank n associated to $\mathcal{U}$ is the set

$$L_{\mathcal{U}} = \{\langle u \rangle_{\mathbb{F}_{q^m}} \mid u \in \mathcal{U} \setminus \{0\}\} \subseteq \mathrm{PG}(k-1, q^m).$$

Rank saturating systems

Definition
An $[n,k]_{q^m/q}$ system $\mathcal{U}$ is **rank ρ-saturating** if $L_{\mathcal{U}}$ is a $(\rho-1)$-saturating set in $\mathrm{PG}(k-1,q^m)$. We call such a linear set a **linear $(\rho-1)$-saturating set**.

rank ρ-saturating systems of $\mathbb{F}_q$-dimension n $\longleftrightarrow$ Duals of $[n,k]_{q^m}$ codes with rank covering radius ρ

Sum-rank saturating systems

Definition

A **sum-rank system** $\mathcal{U}$ is an ordered set $(\mathcal{U}_1, \ldots, \mathcal{U}_t)$, where, for any $i \in \{1, \ldots, t\}$, $\mathcal{U}_i$ is a $\mathbb{F}_q$-subspace of $\mathbb{F}_{q^m}^k$ of dimension n_i, such that $\langle \mathcal{U}_1, \ldots, \mathcal{U}_t \rangle_{\mathbb{F}_{q^m}} = \mathbb{F}_{q^m}^k$.

$\mathcal{U}$ is called an $[\mathbf{n}, k]_{q^m/q}$ **system** if $\mathcal{U}$ has dimension n over $\mathbb{F}_q$.

Definition

$\mathcal{U}$ is **sum-rank ρ-saturating** if $L_{\mathcal{U}_1} \cup \cdots \cup L_{\mathcal{U}_t}$ is $(\rho - 1)$-saturating.

sum-rank ρ-saturating systems of $\mathbb{F}_q$-dimension n $\longleftrightarrow$ Duals of $[\mathbf{n}, k]_{q^m}$ codes with sum-rank covering radius ρ

Characterization and bounds

Characterization

Theorem (B., Borello, Byrne)
Let $\mathcal{U}$ be an $[\mathbf{n}, k]_{q^m/q}$ system and let G be any generator matrix of $\mathcal{U}$. The following are equivalent:

(a) $\mathcal{U}$ is sum-rank ρ-saturating.

(b) For each vector $v \in \mathbb{F}_{q^m}^k$ there exists $\lambda = (\lambda_1, \ldots, \lambda_t)$ such that $\mathrm{wt}_{\mathsf{srk}}(\lambda) \leq \rho$ such that $v = G(\lambda_1, \ldots, \lambda_t)^T$, and ρ is the smallest value with this property.

(c) We have

$$\mathbb{F}_{q^m}^k = \bigcup_{\substack{(\mathcal{S}_i : i \in [t]) :\, \mathcal{S}_i \leq_{\mathbb{F}_q} \mathcal{U}_i, \\ \sum_{i=1}^t \dim_{\mathbb{F}_q} \mathcal{S}_i \leq \rho}} \left(\bigcup_{i=1}^t \langle \mathcal{S}_i \rangle_{\mathbb{F}_{q^m}} \right)$$

and ρ is the smallest integer with this property.

Lower bound

Theorem (B., Borello, Byrne)
Let $\mathcal{U}$ be a sum-rank ρ-saturating $[\mathbf{n}, k]_{q^m/q}$ system. Then

$$q^{m\rho} \sum_{\mathbf{s} \in \mathcal{N}, |\mathbf{s}|=\rho} \begin{bmatrix} \mathbf{n} \\ \mathbf{s} \end{bmatrix}_q \geq q^{mk}.$$

In particular,

$$\frac{1}{4t} \cdot \sum_{1 \leq i < j \leq t} (n_j - n_i)^2 + \frac{\rho(|\mathbf{n}| - \rho)}{t} + 2t \geq m(k - \rho).$$

AALBORG UNIVERSITET

Shortest length

AALBORG UNIVERSITET

Definition

Let t be a positive integer. We define the **shortest length** $s_{q^m/q}(k, \rho, t)$ as the minimal sum of the $\mathbb{F}_q$-dimensions of the $\mathcal{U}_i$, $i \in \{1, \ldots, t\}$, of a sum-rank ρ-saturating system $\mathcal{U} = (\mathcal{U}_1, \ldots, \mathcal{U}_t)$ in $\mathbb{F}_{q^m}^k$.

We define the **homogeneous shortest length** $s_{q^m/q}^{\mathrm{hom}}(k, \rho, t)$ the minimal sum of the $\mathbb{F}_q$-dimensions of the $\mathcal{U}_i$, $i \in \{1, \ldots, t\}$, of a sum-rank ρ-saturating system $\mathcal{U} = (\mathcal{U}_1, \ldots, \mathcal{U}_t)$ in $\mathbb{F}_{q^m}^k$, with the additional hypothesis that they all have equal dimension.

Monotonicity

Proposition (B., Borello, Byrne)
We have that $s_{q^m/q}(k,\rho,t) \leq s_{q^m/q}(k,\rho,t+1)$

Theorem (B., Borello, Byrne)
Let $|\mathbf{n}| > k$. The following hold.

1. $s_{q^m/q}(k,\rho,t) \leq s_{q^m/q}(k,\rho+1,t)$.
2. $s_{q^m/q}(k,\rho,t) \leq s_{q^m/q}(k+1,\rho,t) - 1$.
3. $s_{q^m/q}(k+1,\rho+1,t) \leq s_{q^m/q}(k,\rho+1,t) + 1$.

f-sums

Definition
For each $i \in \{1,2\}$, let $\mathcal{U}^{(i)}$ be an $[\mathbf{n^{(i)}}, k_i]_{q^m/q}$ system, associated with an $[\mathbf{n^{(i)}}, k_i]_{q^m/q}$ sum-rank-metric code $\mathcal{C}_i$. Let $f : \mathbb{F}_{q^m}^{\mathbf{n}^{(1)}} \longrightarrow \mathbb{F}_{q^m}^{\mathbf{n}^{(2)}}$ be an $\mathbb{F}_{q^m}$-linear map. The code

$$\mathcal{C} := \{(u, f(u) + v) : u \in \mathcal{C}_1, v \in \mathcal{C}_2\}$$

is an $[(\mathbf{n^{(1)}}, \mathbf{n^{(2)}}), k_1 + k_2]_{q^m/q}$, which we call the **$f$-sum** of $\mathcal{C}_1$ and $\mathcal{C}_2$. Its associated system is called the **f-sum** of $\mathcal{U}^{(1)}$ and $\mathcal{U}^{(2)}$, which we denote by $\mathcal{U}^{(1)} \oplus_f \mathcal{U}^{(2)}$.

Theorem (B., Borello, Byrne)
$\mathcal{U}^{(1)} \oplus_f \mathcal{U}^{(2)}$ is an $[(\mathbf{n^{(1)}}, \mathbf{n^{(2)}}), k_1 + k_2]_{q^m/q}$ system that is sum-rank-ρ-saturating, where $\rho \leq \rho_1 + \rho_2$. In particular, if $\rho_1 + \rho_2 \leq \min\{k_1 + k_2, m\}$, then

$$s_{q^m/q}(k_1 + k_2, \rho_1 + \rho_2, t_1 + t_2) \leq s_{q^m/q}(k_1, \rho_1, t_1) + s_{q^m/q}(k_2, \rho_2, t_2).$$

AALBORG UNIVERSITET

A construction

Theorem (B., Borello, Byrne)
Let $\mathbb{F}_{q^m} = \mathbb{F}_q[\alpha]$, $r \geq 1$, $h \geq r$ and

$$A_{h,r} := \left[\begin{array}{c|c|c|c|c} I_r & \mathbf{0} & \mathbf{0} & \cdots & \mathbf{0} \\ \hline \mathbf{0} & I_{h-r} & \alpha I_{h-r} & \cdots & \alpha^{m-1} I_{h-r} \end{array}\right]$$

Then

$$G_t := \underbrace{\left[\begin{array}{c|c|c|c} A_{h,r} & \mathbf{0} & \cdots & \mathbf{0} \\ \hline \mathbf{0} & A_{h,r} & \cdots & \mathbf{0} \\ \hline \vdots & \vdots & \ddots & \vdots \\ \hline \mathbf{0} & \mathbf{0} & \cdots & A_{h,r} \end{array}\right]}_{t \text{ times}}$$

generates an homogeneous sum-rank rt-saturating system. So

$$s^{\mathrm{hom}}_{q^m/q}(th, tr, t) \leq t(m(h-r)+r).$$

Constructions

Subgeometries

AALBORG UNIVERSITET

Proposition (B., Borello, Byrne)
Let $\mathcal{P} = \{\mathcal{P}_i\}_{i\in\{1,\dots,t\}}$ a partition of $\mathrm{PG}(k-1,q^m)$ into subspaces. Let k_i be a positive integer such that $\mathcal{P}_i \simeq \mathrm{PG}(k_i-1,q^m)$. If $\mathcal{U}$ is such that each $\mathcal{U}_i$ is rank ρ-saturating in $\mathcal{P}_i$, then $\mathcal{U}$ is sum-rank ρ'-saturating with $\rho' \leq \rho$.

A classic result states that, if $(m,k)=1$, there exists a partition of $\mathrm{PG}(k-1,q^m)$ into $t = \frac{(q^{mk}-1)(q-1)}{(q^m-1)(q^k-1)}$ subgeometries $\mathrm{PG}(k-1,q)$.

This provides an example of an homogeneous 1-saturating system of length $k \cdot \frac{(q^{mk}-1)(q-1)}{(q^m-1)(q^k-1)}$.

Strong Blocking Sets

AALBORG UNIVERSITET

Definition

A subset $\mathcal{M} \subseteq \mathrm{PG}(k-1,q)$ is a **strong blocking set** (or **cutting blocking set**) if for every hyperplane $\mathcal{H}$ of $\mathrm{PG}(k-1,q)$

$$\langle \mathcal{M} \cap \mathcal{H} \rangle = \mathcal{H}.$$

Theorem (Davydov, Giulietti, Marcugini, Pambianco)

Any cutting blocking set in a subgeometry $\mathrm{PG}(k-1,q)$ of $\mathrm{PG}(k-1,q^{k-1})$ is a $(k-2)$-saturating set in $\mathrm{PG}(k-1,q^{k-1})$.

Cutting systems

Definition

A system $\mathcal{U} = (\mathcal{U}_1, \ldots, \mathcal{U}_t) \subset \mathbb{F}_{q^m}^k$ is **cutting** if $L_{\mathcal{U}_1} \cup \ldots \cup L_{\mathcal{U}_t}$ is a strong blocking set in $\mathrm{PG}(k-1, q^m)$, that is if

$$\langle (L_{\mathcal{U}_1} \cup \ldots \cup L_{\mathcal{U}_t}) \cap \mathcal{H} \rangle_{\mathbb{F}_{q^m}} = \mathcal{H},$$

for every hyperplane $\mathcal{H}$ in $\mathrm{PG}(k-1, q^m)$.

Theorem (B., Borello, Byrne)

If $\mathcal{U}$ is a cutting system in $\mathbb{F}_{q^m}^k$, then $\mathcal{U}$ is a sum-rank $(k-1)$-saturating system in $\mathbb{F}_{q^{m(k-1)}}^k$.

AALBORG UNIVERSITET

Thank you for your attention!