Rank distribution of Delsarte codes

Elisa Gorla

Institut de mathématiques, Université de Neuchâtel

Mathematical Coding Theory in Multimedia Streaming
Banff International Research Station
October 15, 2015

Delsarte rank metric codes

Let $1 \leq n \leq m$, $\mathbb{F}_q$ finite field.

Definition

A (Delsarte) rank metric code is an $\mathbb{F}_q$-subspace $0 \neq \mathcal{C} \subset \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$.
The rank distance on $\mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ is

$$d(M,N) = \mathrm{rank}\,(M-N)$$

for $M, N \in \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$.

Delsarte rank metric codes

Let $1 \leq n \leq m$, $\mathbb{F}_q$ finite field.

Definition

A (Delsarte) rank metric code is an $\mathbb{F}_q$-subspace $0 \neq \mathcal{C} \subset \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$.
The rank distance on $\mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ is

$$d(M, N) = \mathrm{rank}\,(M - N)$$

for $M, N \in \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$.

Rank metric codes have applications in:

- network coding,
- distributed storage,
- public-key cryptography.

Gabidulin codes

Definition

A Gabidulin code is an $\mathbb{F}_{q^m}$-subspace $0 \neq C \subset \mathbb{F}_{q^m}^n$.
The rank distance on $\mathbb{F}_{q^m}^n$ is

$$d(u, v) = \dim\langle u_1 - v_1, \ldots, u_n - v_n\rangle_{\mathbb{F}_q}$$

for $u = (u_1, \ldots, u_n), v = (v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n$.

Gabidulin codes

Definition

A Gabidulin code is an $\mathbb{F}_{q^m}$-subspace $0 \neq C \subset \mathbb{F}_{q^m}^n$.
The rank distance on $\mathbb{F}_{q^m}^n$ is

$$d(u, v) = \dim\langle u_1 - v_1, \ldots, u_n - v_n\rangle_{\mathbb{F}_q}$$

for $u = (u_1, \ldots, u_n), v = (v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n$.

Choose a basis $\zeta_1, \ldots, \zeta_m$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, write $u_i = \sum_{j=1}^{m} u_{ij}\zeta_j$. The map

$$\begin{array}{rccc} \zeta: & \mathbb{F}_{q^m}^n & \longrightarrow & \mathrm{Mat}_{n\times m}(\mathbb{F}_q) \\ & u & \longmapsto & (u_{ij}) \end{array}$$

is an invertible linear isometry. Call $\zeta(C)$ a Gabidulin code.

$$\{\text{Gabidulin codes}\} \subseteq \{\text{rank metric codes}\}.$$

Gabidulin codes

Definition

A Gabidulin code is an $\mathbb{F}_{q^m}$-subspace $0 \neq C \subset \mathbb{F}_{q^m}^n$.
The rank distance on $\mathbb{F}_{q^m}^n$ is

$$d(u, v) = \dim\langle u_1 - v_1, \ldots, u_n - v_n\rangle_{\mathbb{F}_q}$$

for $u = (u_1, \ldots, u_n), v = (v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n$.

Choose a basis $\zeta_1, \ldots, \zeta_m$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, write $u_i = \sum_{j=1}^m u_{ij}\zeta_j$. The map

$$\begin{array}{rccc} \zeta: & \mathbb{F}_{q^m}^n & \longrightarrow & \mathrm{Mat}_{n\times m}(\mathbb{F}_q) \\ & u & \longmapsto & (u_{ij}) \end{array}$$

is an invertible linear isometry. Call $\zeta(C)$ a Gabidulin code.

$$\{\text{Gabidulin codes}\} \subsetneq \{\text{rank metric codes}\}.$$

Code equivalence

Theorem (Hua, Wan; Morrison)

Let $f : \mathrm{Mat}_{n\times m}(\mathbb{F}_q) \to \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ *be an* $\mathbb{F}_q$*-linear invertible isometry wrt the rank metric. Then there exist* $A \in \mathrm{GL}_n(\mathbb{F}_q)$, $B \in \mathrm{GL}_m(\mathbb{F}_q)$ *s.t.:*

- $f(M) = AMB$, *or*
- $f(M) = AM^tB$ *(only possible if* $m = n$*).*

Definition

$\mathcal{C}, \mathcal{D} \subset \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ are equivalent if there exists an invertible linear isometry f s.t. $f(\mathcal{C}) = \mathcal{D}$.

Code equivalence

Theorem (Hua, Wan; Morrison)

Let $f : \mathrm{Mat}_{n\times m}(\mathbb{F}_q) \to \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ *be an* $\mathbb{F}_q$*-linear invertible isometry wrt the rank metric. Then there exist* $A \in \mathrm{GL}_n(\mathbb{F}_q)$, $B \in \mathrm{GL}_m(\mathbb{F}_q)$ *s.t.:*

- $f(M) = AMB$, *or*
- $f(M) = AM^tB$ *(only possible if* $m = n$*).*

Definition

$\mathcal{C}, \mathcal{D} \subset \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ are equivalent if there exists an invertible linear isometry f s.t. $f(\mathcal{C}) = \mathcal{D}$.

Equivalent codes have the same invariants and properties, so we study rank metric codes up to equivalence.

Notice that f maps a Gabidulin code to a Gabidulin code.

A MacWilliams Extension Theorem

Theorem (Greferath, Honold, Mc Fadden, Wood, Zumbrägel)

Let $\mathcal{C}, \mathcal{C}'$ be left $\mathrm{Mat}_{n\times n}(\mathbb{F}_q)$-submodules of $\mathrm{Mat}_{n\times nk}(\mathbb{F}_q)$,
$f : \mathcal{C} \to \mathcal{C}'$ invertible linear isometry.
Then f extends to $f : \mathrm{Mat}_{n\times nk}(\mathbb{F}_q) \to \mathrm{Mat}_{n\times nk}(\mathbb{F}_q)$ of the form

$$f([M_1 \ \cdots \ M_k]) = [A_1 M_{\sigma(1)} \ \cdots \ A_k M_{\sigma(k)}]$$

for some permutation σ and $A_1, \ldots, A_k \in \mathrm{GL}_n(\mathbb{F}_q)$.

Recall: $\mathcal{C} \subset \mathrm{Mat}_{n\times nk}(\mathbb{F}_q)$ is a left $\mathrm{Mat}_{n\times n}(\mathbb{F}_q)$-submodule if $[M_1 \ \cdots \ M_k] \in \mathcal{C}$, $A \in \mathrm{Mat}_{n\times n}(\mathbb{F}_q)$, then $[AM_1 \ \cdots \ AM_k] \in \mathcal{C}$.

Example

de la Cruz, Kiermaier, Wassermann, Willems:

- $P \in \mathsf{GL_n}(\mathbb{F}_\mathsf{q})$ of order $q^n - 1$.

Example

de la Cruz, Kiermaier, Wassermann, Willems:

- $P \in \mathrm{GL}_n(\mathbb{F}_q)$ of order $q^n - 1$.
- $Q = P^{q-1}$, Q has order $q^{n-1} + \ldots + q + 1$.

Example

de la Cruz, Kiermaier, Wassermann, Willems:

- $P \in \mathrm{GL_n}(\mathbb{F_q})$ of order $q^n - 1$.
- $Q = P^{q-1}$, Q has order $q^{n-1} + \ldots + q + 1$.
- $\mathcal{C} = \mathbb{F}_q[P] = \{0, I, P, P^2, \ldots, P^{q^n-2}\} \subset \mathrm{Mat_{n\times n}}(\mathbb{F_q})$ is a rank metric code (not a $\mathrm{Mat_{n\times n}}(\mathbb{F_q})$-module).

Example

de la Cruz, Kiermaier, Wassermann, Willems:

- $P \in \mathrm{GL_n}(\mathbb{F_q})$ of order $q^n - 1$.
- $Q = P^{q-1}$, Q has order $q^{n-1} + \ldots + q + 1$.
- $\mathcal{C} = \mathbb{F}_q[P] = \{0, I, P, P^2, \ldots, P^{q^n-2}\} \subset \mathrm{Mat_{n\times n}}(\mathbb{F_q})$ is a rank metric code (not a $\mathrm{Mat_{n\times n}}(\mathbb{F_q})$-module).
- P and Q are linearly independent from I, so there is an $f : \mathcal{C} \to \mathcal{C}$ invertible linear map with $f(I) = I$ and $f(P) = Q$.

Example

de la Cruz, Kiermaier, Wassermann, Willems:

- $P \in \mathrm{GL_n}(\mathbb{F_q})$ of order $q^n - 1$.
- $Q = P^{q-1}$, Q has order $q^{n-1} + \ldots + q + 1$.
- $\mathcal{C} = \mathbb{F}_q[P] = \{0, I, P, P^2, \ldots, P^{q^n-2}\} \subset \mathrm{Mat_{n\times n}}(\mathbb{F_q})$ is a rank metric code (not a $\mathrm{Mat_{n\times n}}(\mathbb{F_q})$-module).
- P and Q are linearly independent from I, so there is an $f : \mathcal{C} \to \mathcal{C}$ invertible linear map with $f(I) = I$ and $f(P) = Q$.
- f is an isometry, since $\operatorname{rank} A = k$ for all $A \in \mathcal{C} \setminus \{0\}$.

Example

de la Cruz, Kiermaier, Wassermann, Willems:

- $P \in \mathrm{GL_n}(\mathbb{F}_q)$ of order $q^n - 1$.
- $Q = P^{q-1}$, Q has order $q^{n-1} + \ldots + q + 1$.
- $\mathcal{C} = \mathbb{F}_q[P] = \{0, I, P, P^2, \ldots, P^{q^n-2}\} \subset \mathrm{Mat_{n\times n}}(\mathbb{F}_q)$ is a rank metric code (not a $\mathrm{Mat_{n\times n}}(\mathbb{F}_q)$-module).
- P and Q are linearly independent from I, so there is an $f : \mathcal{C} \to \mathcal{C}$ invertible linear map with $f(I) = I$ and $f(P) = Q$.
- f is an isometry, since $\operatorname{rank} A = k$ for all $A \in \mathcal{C} \setminus \{0\}$.
- If f can be extended to an invertible linear isometry of $\mathrm{Mat_{n\times n}}(\mathbb{F}_q)$, then $f(M) = AMB$ (or $f(M) = AM^tB$) for some $A, B \in \mathrm{GL_n}(\mathbb{F}_q)$.

Example

de la Cruz, Kiermaier, Wassermann, Willems:

- $P \in \mathrm{GL_n}(\mathbb{F_q})$ of order $q^n - 1$.
- $Q = P^{q-1}$, Q has order $q^{n-1} + \ldots + q + 1$.
- $\mathcal{C} = \mathbb{F}_q[P] = \{0, I, P, P^2, \ldots, P^{q^n-2}\} \subset \mathrm{Mat_{n\times n}}(\mathbb{F_q})$ is a rank metric code (not a $\mathrm{Mat_{n\times n}}(\mathbb{F_q})$-module).
- P and Q are linearly independent from I, so there is an $f : \mathcal{C} \to \mathcal{C}$ invertible linear map with $f(I) = I$ and $f(P) = Q$.
- f is an isometry, since $\operatorname{rank} A = k$ for all $A \in \mathcal{C} \setminus \{0\}$.
- If f can be extended to an invertible linear isometry of $\mathrm{Mat_{n\times n}}(\mathbb{F_q})$, then $f(M) = AMB$ (or $f(M) = AM^tB$) for some $A, B \in \mathrm{GL_n}(\mathbb{F_q})$.
- Since $f(I) = I$, then $B = A^{-1}$ and $Q = APA^{-1}$ (or $Q = AP^tA^{-1}$).

Example

de la Cruz, Kiermaier, Wassermann, Willems:

- $P \in \mathrm{GL_n}(\mathbb{F_q})$ of order $q^n - 1$.
- $Q = P^{q-1}$, Q has order $q^{n-1} + \ldots + q + 1$.
- $\mathcal{C} = \mathbb{F}_q[P] = \{0, I, P, P^2, \ldots, P^{q^n-2}\} \subset \mathrm{Mat_{n\times n}}(\mathbb{F_q})$ is a rank metric code (not a $\mathrm{Mat_{n\times n}}(\mathbb{F_q})$-module).
- P and Q are linearly independent from I, so there is an $f : \mathcal{C} \to \mathcal{C}$ invertible linear map with $f(I) = I$ and $f(P) = Q$.
- f is an isometry, since $\operatorname{rank} A = k$ for all $A \in \mathcal{C} \setminus \{0\}$.
- If f can be extended to an invertible linear isometry of $\mathrm{Mat_{n\times n}}(\mathbb{F_q})$, then $f(M) = AMB$ (or $f(M) = AM^tB$) for some $A, B \in \mathrm{GL_n}(\mathbb{F_q})$.
- Since $f(I) = I$, then $B = A^{-1}$ and $Q = APA^{-1}$ (or $Q = AP^tA^{-1}$).
- This is not possible, since $\operatorname{rank}(APA^{-1}) = \operatorname{rank}(AP^tA^{-1}) = q^n - 1$.

Code duality

Definition

The dual of $\mathcal{C}$ is $\mathcal{C}^\perp = \{M \in \mathrm{Mat}_{n\times m}(\mathbb{F}_q) \mid \mathrm{Tr}(MN^t) = 0 \text{ for all } N \in \mathcal{C}\}$.

Since $(M, N) \mapsto \mathrm{Tr}(MN^t)$ is a scalar product, then:

- $\dim \mathcal{C}^\perp = mn - \dim \mathcal{C}$,
- $(\mathcal{C} + \mathcal{D})^\perp = \mathcal{C}^\perp \cap \mathcal{D}^\perp$ and $(\mathcal{C} \cap \mathcal{D})^\perp = \mathcal{C}^\perp + \mathcal{D}^\perp$,
- $(\mathcal{C}^\perp)^\perp = \mathcal{C}$.

Code duality

Definition

The dual of $\mathcal{C}$ is $\mathcal{C}^\perp = \{M \in \mathrm{Mat}_{n\times m}(\mathbb{F}_q) \mid \mathrm{Tr}(MN^t) = 0 \text{ for all } N \in \mathcal{C}\}$.

Since $(M, N) \mapsto \mathrm{Tr}(MN^t)$ is a scalar product, then:

- $\dim \mathcal{C}^\perp = mn - \dim \mathcal{C}$,
- $(\mathcal{C} + \mathcal{D})^\perp = \mathcal{C}^\perp \cap \mathcal{D}^\perp$ and $(\mathcal{C} \cap \mathcal{D})^\perp = \mathcal{C}^\perp + \mathcal{D}^\perp$,
- $(\mathcal{C}^\perp)^\perp = \mathcal{C}$.

Remark

The scalar product on $\mathbb{F}_{q^m}^n$ $u \bullet v = \sum_{i=1}^n u_i v_i$ allows us to define the dual of a Gabidulin code $C \subset \mathbb{F}_{q^m}^n$ as

$$C^* = \{u \in \mathbb{F}_{q^m}^n \mid u \bullet v = 0 \text{ for all } v \in C\}.$$

Question: Is $\zeta(C^*) = \zeta(C)^\perp$?

$C \subset \mathbb{F}_{q^m}^n$ a Gabidulin code, $\mathcal{C} \subset \mathrm{Mat}_{\mathsf{n}\times\mathsf{m}}(\mathbb{F}_{\mathsf{q}})$ a Delsarte code, define:

$$\mathcal{C}^{\perp} = \{M \in \mathrm{Mat}_{\mathsf{n}\times\mathsf{m}}(\mathbb{F}_{\mathsf{q}}) \mid \mathrm{Tr}(MN^t) = 0 \text{ for all } N \in \mathcal{C}\}$$

$$C^* = \{u \in \mathbb{F}_{q^m}^n \mid u \bullet v = 0 \text{ for all } v \in C\}.$$

$C \subset \mathbb{F}_{q^m}^n$ a Gabidulin code, $\mathcal{C} \subset \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ a Delsarte code, define:

$$\mathcal{C}^\perp = \{M \in \mathrm{Mat}_{n\times m}(\mathbb{F}_q) \mid \mathrm{Tr}(MN^t) = 0 \text{ for all } N \in \mathcal{C}\}$$

$$C^* = \{u \in \mathbb{F}_{q^m}^n \mid u \bullet v = 0 \text{ for all } v \in C\}.$$

In general $\zeta(C^*) \neq \zeta(C)^\perp$.

$C \subset \mathbb{F}_{q^m}^n$ a Gabidulin code, $\mathcal{C} \subset \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ a Delsarte code, define:

$$\mathcal{C}^\perp = \{M \in \mathrm{Mat}_{n\times m}(\mathbb{F}_q) \mid \mathrm{Tr}(MN^t) = 0 \text{ for all } N \in \mathcal{C}\}$$

$$C^* = \{u \in \mathbb{F}_{q^m}^n \mid u \bullet v = 0 \text{ for all } v \in C\}.$$

In general $\zeta(C^*) \neq \zeta(C)^\perp$.

Definition

Two bases $\zeta = \{\zeta_1, \ldots, \zeta_m\}$ and $\zeta' = \{\zeta'_1, \ldots, \zeta'_m\}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ are dual if $\mathrm{Tr}(\zeta_i \zeta'_j) = \delta_{ij}$ for all i, j.

Theorem (Ravagnani)

Let $C \subset \mathbb{F}_{q^m}^n$ be a Gabidulin code, ζ, ζ' be dual bases. Then

$$\zeta'(C^*) = \zeta(C)^\perp.$$

$C \subset \mathbb{F}_{q^m}^n$ a Gabidulin code, $\mathcal{C} \subset \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ a Delsarte code, define:

$$\mathcal{C}^\perp = \{M \in \mathrm{Mat}_{n\times m}(\mathbb{F}_q) \mid \mathrm{Tr}(MN^t) = 0 \text{ for all } N \in \mathcal{C}\}$$

$$C^* = \{u \in \mathbb{F}_{q^m}^n \mid u \bullet v = 0 \text{ for all } v \in C\}.$$

In general $\zeta(C^*) \neq \zeta(C)^\perp$.

Definition

Two bases $\zeta = \{\zeta_1, \ldots, \zeta_m\}$ and $\zeta' = \{\zeta'_1, \ldots, \zeta'_m\}$ of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$ are dual if $\mathrm{Tr}(\zeta_i \zeta'_j) = \delta_{ij}$ for all i, j.

Theorem (Ravagnani)

Let $C \subset \mathbb{F}_{q^m}^n$ be a Gabidulin code, ζ, ζ' be dual bases. Then

$$\zeta'(C^*) = \zeta(C)^\perp.$$

Take home message: Up to code equivalence, studying duals of rank metric codes we automatically study duals of Gabidulin codes.

MacWilliams identities

$\mathcal{C} \subset \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ Delsarte code, $\mathcal{C}^\perp$ its dual.

Define $\begin{bmatrix} a \\ b \end{bmatrix} = \frac{(q^a-1)(q^{a-1}-1)\cdots(q^{a-b+1})}{(q^b-1)(q^{b-1}-1)\cdots(q-1)}$.

Definition

The rank distribution is the collection of the rank weights

$$A_j(\mathcal{C}) = |\{M \in \mathcal{C} \mid \operatorname{rank} M = j\}|.$$

Theorem (Delsarte)

$$A_j(\mathcal{C}^\perp) = \frac{1}{|\mathcal{C}|}\sum_{i=0}^{n} A_i(\mathcal{C}) \sum_{s=0}^{n} (-1)^{j-s} q^{sm+\binom{j-s}{2}} \begin{bmatrix} n-s \\ n-j \end{bmatrix} \begin{bmatrix} n-i \\ s \end{bmatrix}$$

for $j = 0, \ldots, n$.

Different proofs of the MacWilliams identities were given by Delsarte, Gaduleau and Yan, Gluesing-Luerssen, Ravagnani.

Minimum rank distance and Singleton bound

Definition

The minimum rank distance of $\mathcal{C} \subset \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ is

$$d = \min\{\operatorname{rank} M \mid M \in \mathcal{C}\}.$$

The dimension of $\mathcal{C}$ is $t = \dim_{\mathbb{F}_q} \mathcal{C}$.

Remark

If $C \subset \mathbb{F}_{q^m}^n$ is a Gabidulin code, then $m \mid t = \dim_{\mathbb{F}_q}(\zeta(C)) = m \dim_{\mathbb{F}_{q^m}}(C)$.

Minimum rank distance and Singleton bound

Definition

The minimum rank distance of $\mathcal{C} \subset \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ is

$$d = \min\{\operatorname{rank} M \mid M \in \mathcal{C}\}.$$

The dimension of $\mathcal{C}$ is $t = \dim_{\mathbb{F}_q} \mathcal{C}$.

Remark

If $C \subset \mathbb{F}_{q^m}^n$ is a Gabidulin code, then $m \mid t = \dim_{\mathbb{F}_q}(\zeta(C)) = m \dim_{\mathbb{F}_{q^m}}(C)$.

Theorem (Delsarte)

We have $t \leq m(n-d+1)$, and the bound is sharp.

Definition

A code $\mathcal{C}$ is MRD if $t = m(n-d+1)$.

Constructions of MRD codes

Gabidulin: $g_1, \ldots, g_m \in \mathbb{F}_{q^m}$ linearly independent over $\mathbb{F}_q$, $\gcd\{k, m\} = 1$.
$G = (g_j^{q^{k(i-1)}})_{1 \le i \le n-d+1,\ 1 \le j \le n} \in \mathrm{Mat}_{n \times (n-d+1)}(\mathbb{F}_{q^m})$. The code
$C = \mathbb{F}_{q^m}^{n-d+1} G \subset \mathbb{F}_{q^m}^n$ is MRD (equivalently, $\zeta(C) \subset \mathrm{Mat}_{\mathsf{n} \times \mathsf{m}}(\mathbb{F}_{\mathsf{q}})$ is MRD).

Constructions of MRD codes

Delsarte: $\zeta_1, \ldots, \zeta_m$ basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, $\mu_1, \ldots, \mu_n \in \mathbb{F}_{q^m}$ linearly independent over $\mathbb{F}_q$. The code

$$\left\{ \left(\mathrm{Tr}\left(\sum_{s=0}^{n-d} u_s \mu_i^{q^s} \zeta_j \right) \right)_{1 \le i \le n,\ 1 \le j \le m} \middle| \ (u_0, \ldots, u_{n-d}) \in \mathbb{F}_{q^m}^{n-d+1} \right\}$$

is MRD.

Gabidulin: $g_1, \ldots, g_m \in \mathbb{F}_{q^m}$ linearly independent over $\mathbb{F}_q$, $\gcd\{k, m\} = 1$. $G = (g_j^{q^{k(i-1)}})_{1 \le i \le n-d+1,\ 1 \le j \le n} \in \mathrm{Mat}_{n \times (n-d+1)}(\mathbb{F}_{q^m})$. The code $C = \mathbb{F}_{q^m}^{n-d+1} G \subset \mathbb{F}_{q^m}^n$ is MRD (equivalently, $\zeta(C) \subset \mathrm{Mat}_{n \times m}(\mathbb{F}_q)$ is MRD).

MRD codes and their duals

$\mathcal{C} \subset \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ with min rank d, $\mathcal{C}^\perp \subset \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ with min rank $d^\perp$.

Corollary (Delsarte)

$\mathcal{C}$ is MRD iff $\mathcal{C}^\perp$ is MRD.

MRD codes and their duals

$\mathcal{C} \subset \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ with min rank d, $\mathcal{C}^\perp \subset \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ with min rank $d^\perp$.

Corollary (Delsarte)

$\mathcal{C}$ is MRD iff $\mathcal{C}^\perp$ is MRD.

The MacWilliams identities can be rewritten in the form

$$\sum_{i=0}^{n-s} A_i(\mathcal{C}) \begin{bmatrix} n-i \\ s \end{bmatrix} = q^{m(n-d+1-s)} \sum_{j=0}^{s} A_i(\mathcal{C}^\perp) \begin{bmatrix} n-j \\ s-j \end{bmatrix}$$

for $s = 0, \ldots, n$.

Corollary (Delsarte)

The rank distribution of an MRD code is determined by its parameters m, n, d.

Rank defect

The results which follow are joint work with J. de la Cruz, H. H. López, and A. Ravagnani.

$\mathcal{C} \subset \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ rank metric code of minimum rank distance d, $t = \dim \mathcal{C}$.

Definition

The rank defect of $\mathcal{C}$ is

$$\mathrm{Rdef}(\mathcal{C}) = n - \left\lceil \frac{t}{m} \right\rceil - d + 1.$$

Rank defect

The results which follow are joint work with J. de la Cruz, H. H. López, and A. Ravagnani.

$\mathcal{C} \subset \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ rank metric code of minimum rank distance d, $t = \dim \mathcal{C}$.

Definition

The rank defect of $\mathcal{C}$ is

$$\mathrm{Rdef}(\mathcal{C}) = n - \left\lceil \frac{t}{m} \right\rceil - d + 1.$$

Remarks:

- by the Singleton bound $d \leq n - \left\lceil \frac{t}{m} \right\rceil + 1$, so $\mathrm{Rdef}(\mathcal{C}) \geq 0$,
- if $\mathcal{C}$ is MRD, then $\mathrm{Rdef}(\mathcal{C}) = 0$,
- there are non MRD codes $\mathcal{C}$ with $\mathrm{Rdef}(\mathcal{C}) = 0$ for all n, m, t s.t. $m \nmid t$.

Quasi-MRD codes

Definition

A code $\mathcal{C}$ is Quasi-MRD or QMRD if it is not MRD and $d = n - \left\lceil \frac{t}{m} \right\rceil + 1$, i.e. if it is not MRD and $\mathrm{Rdef}(\mathcal{C}) = 0$.

Quasi-MRD codes

Definition

A code $\mathcal{C}$ is Quasi-MRD or QMRD if it is not MRD and $d = n - \left\lceil \frac{t}{m} \right\rceil + 1$, i.e. if it is not MRD and $\mathrm{Rdef}(\mathcal{C}) = 0$.

Example

$q = 2$, $n = m = 3$, let

$$\mathcal{C} = \left\langle \begin{bmatrix} 0 & 1 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix} \right\rangle.$$

Then $t = \dim \mathcal{C} = 4$ and $d = 2$, so $\mathcal{C}$ is QMRD.
However $\mathcal{C}^\perp$ is not QMRD, since $d^\perp = 1$ as

$$\begin{bmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \in \mathcal{C}^\perp.$$

Dually QMRD codes

Definition

A code $\mathcal{C}$ is dually QMRD if both $\mathcal{C}$ and $\mathcal{C}^{\perp}$ are QMRD.

Dually QMRD codes

Definition

A code $\mathcal{C}$ is dually QMRD if both $\mathcal{C}$ and $\mathcal{C}^{\perp}$ are QMRD.

Example

Any $\mathcal{C} \subset \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ with $0 < t = \dim \mathcal{C} < m$ with $d < n$ is not QMRD.

Since $m(n-1) < \dim \mathcal{C}^{\perp} < mn$, then $d^{\perp} = 1$ and $\mathcal{C}^{\perp}$ is QMRD.

Remarks: For any q:

- if $m = 1$ there are no QMRD codes,
- if $m \geq 2$ there are QMRD codes which are not dually QMRD.

Dually QMRD codes

Definition

A code $\mathcal{C}$ is dually QMRD if both $\mathcal{C}$ and $\mathcal{C}^\perp$ are QMRD.

Example

Any $\mathcal{C} \subset \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ with $0 < t = \dim \mathcal{C} < m$ with $d < n$ is not QMRD.

Since $m(n-1) < \dim \mathcal{C}^\perp < mn$, then $d^\perp = 1$ and $\mathcal{C}^\perp$ is QMRD.

Remarks: For any q:

- if $m = 1$ there are no QMRD codes,
- if $m \geq 2$ there are QMRD codes which are not dually QMRD.

Proposition

Let $\mathcal{C}$ be QMRD, $t = \dim \mathcal{C} = sm + r$, $0 < r < m$. Then $\mathcal{C}^\perp$ is QMRD iff

$$A_d(\mathcal{C}) = \begin{bmatrix} n \\ d \end{bmatrix} (q^s - 1).$$

MRD and dually QMRD codes

$\mathcal{C} \subset \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ with minimum rank d and $t = \dim \mathcal{C}$,
$\mathcal{C}^\perp \subset \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ with minimum rank $d^\perp$.

Proposition

- *If* $t \mid m$, *then* $d + d^\perp = n + 2$ *or* $d + d^\perp \leq n$.
- *If* $t \nmid m$, *then* $d + d^\perp \leq n + 1$.

MRD and dually QMRD codes

$\mathcal{C} \subset \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ with minimum rank d and $t = \dim \mathcal{C}$,
$\mathcal{C}^\perp \subset \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ with minimum rank $d^\perp$.

Proposition

- *If* $t \mid m$, *then* $d + d^\perp = n + 2$ *or* $d + d^\perp \leq n$.
- *If* $t \nmid m$, *then* $d + d^\perp \leq n + 1$.

Proposition

- $\mathcal{C}$ *is MRD iff* $d + d^\perp = n + 2$.
- $\mathcal{C}$ *is dually QMRD iff* $d + d^\perp = n + 1$.

Higher rank weights and dual rank defect

Definition

An optimal anticode $\mathcal{A} \subseteq \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ is a rank metric code of $\dim \mathcal{A} = m \cdot \mathrm{maxrank}(\mathcal{A})$, where $\mathrm{maxrank}(\mathcal{A}) = \max\{\mathrm{rank}\, M \mid M \in \mathcal{A}\}$.

The higher rank weights of $\mathcal{C}$ are

$$a_k(\mathcal{C}) = \frac{1}{m} \min\{\dim(\mathcal{A}) \mid \mathcal{A} \subseteq \mathrm{Mat}_{n\times m}(\mathbb{F}_q) \text{ optimal anticode, } \dim(\mathcal{A} \cap \mathcal{C}) \geq k\}$$

for $1 \leq k \leq t = \dim \mathcal{C}$.

Higher rank weights and dual rank defect

Definition

An optimal anticode $\mathcal{A} \subseteq \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ is a rank metric code of $\dim \mathcal{A} = m \cdot \mathrm{maxrank}(\mathcal{A})$, where $\mathrm{maxrank}(\mathcal{A}) = \max\{\mathrm{rank}\, M \mid M \in \mathcal{A}\}$.

The higher rank weights of $\mathcal{C}$ are

$$a_k(\mathcal{C}) = \frac{1}{m}\min\{\dim(\mathcal{A}) \mid \mathcal{A} \subseteq \mathrm{Mat}_{n\times m}(\mathbb{F}_q) \text{ optimal anticode, } \dim(\mathcal{A}\cap\mathcal{C}) \geq k\}$$

for $1 \leq k \leq t = \dim \mathcal{C}$.

Proposition

$\mathcal{C} \subset \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ with min rank d and $t = \dim \mathcal{C}$. If $t < m$, then $d^\perp = 0$ and $\mathrm{Rdef}(\mathcal{C}^\perp) = 0$. *If $t \geq m$, write $t = sm + r$, $0 \leq r < m$. Then*

$$d^\perp = \begin{cases} s+1 & \text{if } n+1-a_{r+1}(\mathcal{C}) = s \\ \min\{1 \leq k \leq s \mid n+1-a_{t+1-km}(\mathcal{C}) > k\} & \text{else,} \end{cases}$$

and $\mathrm{Rdef}(\mathcal{C}^\perp) = s+1-d^\perp$.

Higher rank weights of MRD and dually QMRD codes

$\mathcal{C} \subset \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ with min rank d and $t = \dim \mathcal{C} = sm + r$, $0 \leq r < m$.

Corollary

The following are equivalent:

- $\mathcal{C}$ *is MRD or dually QMRD,*
- $a_{r+1}(\mathcal{C}) = n - s + 1$,
- $a_k(\mathcal{C}) = n - s + \left\lceil \frac{k-r}{m} \right\rceil$ *for* $k \geq r + 1$.

In particular, $\mathcal{C}$ is MRD iff $a_1(\mathcal{C}) = n - s + 1$
iff $a_k(\mathcal{C}) = n - s + \left\lceil \frac{k}{m} \right\rceil$ for $k \geq r + 1$.

Rank distribution

$\mathcal{C} \subset \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ with minimum rank d and $t = \dim \mathcal{C}$,
$\mathcal{C}^\perp \subset \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ with minimum rank $d^\perp$.

Theorem

Let $\delta = 1$ if $\mathcal{C}$ is MRD, and $\delta = 0$ otherwise. Then

$$\begin{aligned} A_{n-d^\perp+k}(\mathcal{C}) &= (-1)^k q^{\binom{k}{2}} \sum_{j=d^\perp}^{n-d} \begin{bmatrix} j \\ d^\perp - k \end{bmatrix} \begin{bmatrix} j-d^\perp+k-1 \\ k-1 \end{bmatrix} A_{n-j}(\mathcal{C}) \\ &\quad + \begin{bmatrix} n \\ d^\perp - k \end{bmatrix} \sum_{i=0}^{k-1-\delta} (-1)^i q^{\binom{i}{2}} \begin{bmatrix} n-d^\perp+k \\ i \end{bmatrix} \left(q^{t-m(d^\perp-k+i)} - 1 \right). \end{aligned}$$

for $1 \le k \le d^\perp$.

The rank distribution of $\mathcal{C}$ is determined by $n, m, t, d, d^\perp$, and the weights $A_d(\mathcal{C}), \ldots, A_{n-d^\perp}(\mathcal{C})$.

Rank distribution of dually QMRD codes

Corollary

Let $\mathcal{C}$ be MRD or dually QMRD. Then

$$A_k(\mathcal{C}) = \begin{bmatrix} n \\ k \end{bmatrix} \sum_{i=0}^{k-n+\lceil \frac{t}{m} \rceil - 1} (-1)^i q^{\binom{i}{2}} \begin{bmatrix} k \\ i \end{bmatrix} \left(q^{t-m(n+i-k)} - 1 \right)$$

for $d = n - \left\lceil \frac{t}{m} \right\rceil + 1 \leq k \leq n$. In particular, the rank distribution of $\mathcal{C}$ is determined by n, m, and t.

Rank distribution of dually QMRD codes

Corollary

Let $\mathcal{C}$ be MRD or dually QMRD. Then

$$A_k(\mathcal{C}) = \begin{bmatrix} n \\ k \end{bmatrix} \sum_{i=0}^{k-n+\lceil \frac{t}{m} \rceil - 1} (-1)^i q^{\binom{i}{2}} \begin{bmatrix} k \\ i \end{bmatrix} \left(q^{t-m(n+i-k)} - 1 \right)$$

for $d = n - \left\lceil \frac{t}{m} \right\rceil + 1 \leq k \leq n$. In particular, the rank distribution of $\mathcal{C}$ is determined by n, m, and t.

Example

Let $2 \leq n \leq m$, $t = \dim \mathcal{C} = nm - 1$. Then $d = 1$ and $\mathcal{C}$ is QMRD, but not dually QMRD. Moreover, $A_1(\mathcal{C})$ depends on $d^\perp$:

$$A_1(\mathcal{C}) = \frac{q^{m+n-1} + q^{m+n-d^\perp} - q^{m+n-d^\perp-1} - q^m - q^n + 1}{q-1}.$$

Codes with small rank defect

$\mathcal{C} \subset \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ with minimum rank d and $t = \dim \mathcal{C}$,
$\mathcal{C}^\perp \subset \mathrm{Mat}_{n\times m}(\mathbb{F}_q)$ with minimum rank $d^\perp$.

Theorem

If $d + d^\perp = n$ *and* $m \mid t$, *then* $\mathrm{Rdef}(\mathcal{C}) = \mathrm{Rdef}(\mathcal{C}^\perp) = 1$ *and*

$$A_d(\mathcal{C}) = A_{d^\perp}(\mathcal{C}^\perp).$$

Remark

If $d + d^\perp = n$ and $m \nmid t$, then $\mathrm{Rdef}(\mathcal{C}) + \mathrm{Rdef}(\mathcal{C}^\perp) = 1$.

Conclusions

Main topics discussed in this talk:

- Gabidulin codes are special rank metric codes,
- code equivalence and the MacWilliams Extension Theorem,
- duality and MacWilliams identities,
- MRD, QMRD, and dually QMRD codes,
- higher rank weights of MRD and dually QMRD codes,
- rank distribution of dually QMRD codes,
- codes with large minimum rank.

Conclusions

Main topics discussed in this talk:

- Gabidulin codes are special rank metric codes,
- code equivalence and the MacWilliams Extension Theorem,
- duality and MacWilliams identities,
- MRD, QMRD, and dually QMRD codes,
- higher rank weights of MRD and dually QMRD codes,
- rank distribution of dually QMRD codes,
- codes with large minimum rank.

Thank you for your attention!

References:

- J. de la Cruz, M. Kiermaier, A. Wassermann, W. Willems, Algebraic structures of MRD codes, arXiv:1502.02711
- P. Delsarte, Bilinear forms over a finite field with applications to coding theory, J. Comb. Theory, Ser. A 25, 226–241 (1978)
- J. de la Cruz, E. Gorla, H. H. López, A. Ravagnani, Rank distribution of Delsarte codes, arXiv:1510.01008
- E. M. Gabidulin, Theory of codes with maximum rank distance, Problems on Information Transmission 21 (1), 1–12 (1985)
- M. Gaduleau, Z. Yan, MacWilliams Identities for the Rank Metric, ISIT 2007 (Nice, France), 36–40
- H. Gluesing-Luerssen, Fourier-Reflexive Partitions and MacWilliams Identities for Additive Codes, Des. Codes Cryptogr. 75, 543–563 (2015)
- M. Greferath, T. Honold, C. Mc Fadden, J. A. Wood, J. Zumbrägel, MacWilliams' Extension Theorem for Bi-Invariant Weights over Finite Principal Ideal Rings, arXiv:1309.3292
- A. Ravagnani, Rank-metric codes and their duality theory, arXiv:1410.1333 (to appear on Des. Codes Cryptogr.)
- A. Ravagnani, Generalized weights: an anticode approach, arXiv:1410.7207