The Critical Problem for Rank-Metric Codes

Gianira N. Alfarano

OpeRa 2024 - Open Problems on Rank-Metric Codes
Università degli Studi della Campania, Luigi Vanvitelli
February 16th, 2024

Overview

Contents

The Critical Problem

Definition (Crapo & Rota 1970)

Let $S \subseteq \mathbb{F}_q^k \setminus \{0\}$. Let $\mathcal{F} = (f_1, \dots, f_r)$ be a list of linear functionals $f_i : \mathbb{F}_q^k \to \mathbb{F}_q$. We say that $\mathcal{F}$ **distinguishes** S if for all $v \in S$, $v \notin \cap_{i=1}^r \ker f_i$, i.e.

$$\forall v \in S, \quad \exists\, i \in \{1, \dots, r\}, \text{ s.t. } f_i(v) \neq 0.$$

H. Crapo, G. Rota. "On The Foundations of Combinatorial Theory: Combinatorial Geometries.", 1970.

Problem (The Critical Problem)

What is the minimum number of linear forms that distinguishes S?

The Critical Problem

Definition (Crapo & Rota 1970)

Let $S \subseteq \mathrm{PG}(k-1,q)$. Let $\mathcal{H} = (H_1, \dots, H_r)$ be some hyperplanes. We say that $\mathcal{H}$ **distinguishes** S if for all $P \in S$, $P \notin \cap_{i=1}^{r} H_i$.

H. Crapo, G. Rota. "On The Foundations of Combinatorial Theory: Combinatorial Geometries.", 1970.

Problem (The Critical Problem)

What is the minimum number of hyperplanes in $\mathrm{PG}(k-1,q)$ *distinguishing* S*?*

The Critical Problem

Definition (Crapo & Rota 1970)

Let $S \subseteq \mathrm{PG}(k-1,q)$. Let $\mathcal{H} = (H_1, \dots, H_r)$ be some hyperplanes. We say that $\mathcal{H}$ **distinguishes** S if for all $P \in S$, $P \notin \cap_{i=1}^{r} H_i$.

H. Crapo, G. Rota. "On The Foundations of Combinatorial Theory: Combinatorial Geometries.", 1970.

Problem (The Critical Problem)

What is the minimum number of hyperplanes in $\mathrm{PG}(k-1,q)$ *distinguishing* S*?*

- **Critical Theorem**: Theoretical solution to the critical problem.
- **Critical Exponent**: The number that we look for in the critical problem.

The Critical Problem

Definition (Crapo & Rota 1970)

Let $S \subseteq \mathrm{PG}(k-1, q)$. Let $\mathcal{H} = (H_1, \dots, H_r)$ be some hyperplanes. We say that $\mathcal{H}$ **distinguishes** S if for all $P \in S$, $P \notin \cap_{i=1}^r H_i$.

H. Crapo, G. Rota. "On The Foundations of Combinatorial Theory: Combinatorial Geometries.", 1970.

Problem (The Critical Problem)

What is the minimum number of hyperplanes in $\mathrm{PG}(k-1, q)$ *distinguishing* S*?*

- **Critical Theorem**: Theoretical solution to the critical problem.
- **Critical Exponent**: The number that we look for in the critical problem.

Contributors: Britz, Dowling, Green, Gruica, Imamura, Jany, Kung, Oxley, Ravagnani, Sheekey, Shiromoto, Tutte, Welsh, White, Whittle, Zullo...

q-Analogues

Finite set $\longrightarrow$ finite dimensional vector space over the finite field $\mathbb{F}_q$.

Classic	q-**Analogues**
$\{1\ldots,n\}$	$\mathbb{F}_q^n$
element	1-dim subspace
size	dimension
intersection	intersection
union	sum
complement	orthogonal complement

q-Analogues

Finite set $\longrightarrow$ finite dimensional vector space over the finite field $\mathbb{F}_q$.

Classic	q-**Analogues**
$\{1\ldots,n\}$	$\mathbb{F}_q^n$
element	1-dim subspace
size	dimension
intersection	intersection
union	sum
complement	orthogonal complement

From q-analogue to "classic": let $q \to 1$.

q-Analogues

Finite set $\longrightarrow$ finite dimensional vector space over the finite field $\mathbb{F}_q$.

Classic	q-**Analogues**
$\{1\ldots,n\}$	$\mathbb{F}_q^n$
element	1-dim subspace
size	dimension
intersection	intersection
union	sum
complement	orthogonal complement

From q-analogue to "classic": let $q \to 1$.

Example:

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

$$\begin{bmatrix} n \\ k \end{bmatrix}_q = \frac{(q^n-1)(q^{n-1}-1)\cdots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\cdots(q-1)}$$

Contents

Linear Hamming-Metric Codes

Basic Notions

- $\mathbb{F}_q$ finite field of order q.
- $E := \mathbb{F}_q^n$.
- $[n] := \{1, \ldots, n\}$.

Linear Hamming-Metric Codes

Basic Notions

- $\mathbb{F}_q$ finite field of order q.
- $E := \mathbb{F}_q^n$.
- $[n] := \{1, \ldots, n\}$.
- The **Hamming distance** between $u, v \in E$ is $d_{\mathrm{H}}(u, v) := |\{i : u_i \neq v_i\}|$.
- The **support** of $u \in E$ is $\mathrm{supp}(u) := \{i : u_i \neq 0\}$.
- The **Hamming weight** of $u \in E$ is $\mathrm{wt}_{\mathrm{H}}(u) := |\mathrm{supp}(u)| = d_{\mathrm{H}}(u, 0)$.

Linear Hamming-Metric Codes

Basic Notions

- $\mathbb{F}_q$ finite field of order q.
- $E := \mathbb{F}_q^n$.
- $[n] := \{1, \ldots, n\}$.
- The **Hamming distance** between $u, v \in E$ is $d_{\mathrm{H}}(u, v) := |\{i : u_i \neq v_i\}|$.
- The **support** of $u \in E$ is $\mathrm{supp}(u) := \{i : u_i \neq 0\}$.
- The **Hamming weight** of $u \in E$ is $\mathrm{wt}_{\mathrm{H}}(u) := |\mathrm{supp}(u)| = d_{\mathrm{H}}(u, 0)$.

An $[n, k]_q$ **linear code** C is a k-dimensional subspace of $\mathbb{F}_q^n$.

- $\mathrm{supp}(C) = \bigcup_{c \in C} \mathrm{supp}(c)$.
- C is **non-degenerate** if $\mathrm{supp}(C) = [n]$.

Linear Hamming-Metric Codes

Basic Notions

- $\mathbb{F}_q$ finite field of order q.
- $E := \mathbb{F}_q^n$.
- $[n] := \{1, \ldots, n\}$.
- The **Hamming distance** between $u, v \in E$ is $d_{\mathrm{H}}(u, v) := |\{i : u_i \neq v_i\}|$.
- The **support** of $u \in E$ is $\mathrm{supp}(u) := \{i : u_i \neq 0\}$.
- The **Hamming weight** of $u \in E$ is $\mathrm{wt}_{\mathrm{H}}(u) := |\mathrm{supp}(u)| = d_{\mathrm{H}}(u, 0)$.

An $[n, k]_q$ **linear code** C is a k-dimensional subspace of $\mathbb{F}_q^n$.

- $\mathrm{supp}(C) = \bigcup_{c \in C} \mathrm{supp}(c)$.
- C is **non-degenerate** if $\mathrm{supp}(C) = [n]$.
- For $S \subseteq [n]$, $C(S) := \{c \in C : \mathrm{supp}(c) \subseteq \bar{S}\}$ is called a **shortened subcode** of C.
- $C = \mathrm{rowsp}(G) = \{uG \mid u \in \mathbb{F}_q^k\}$, where $G \in \mathbb{F}_q^{k \times n}$ is a **generator matrix**.

Rank-Metric Codes

Basic Notions

- An $\mathbb{F}_q$-$[n \times m, k, d]$ **rank-metric code** C is a k-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_q^{n\times m}$.
- The **minimum rank distance** of C is $d := \min\{\mathrm{rk}(M) : 0 \neq M \in C\}$.

Rank-Metric Codes

Basic Notions

- An $\mathbb{F}_q$-$[n \times m, k, d]$ **rank-metric code** C is a k-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_q^{n \times m}$.
- The **minimum rank distance** of C is $d := \min\{\mathrm{rk}(M) : 0 \neq M \in C\}$.
- For every $M \in C$, $\mathrm{supp}(M) := \mathrm{colsp}(M) \leq \mathbb{F}_q^n$.
- $\mathrm{supp}(C) := \sum_{M \in C} \mathrm{supp}(M)$.
- C is **non-degenerate** if $\mathrm{supp}(C) = E$.

Rank-Metric Codes

Basic Notions

- An $\mathbb{F}_q$-$[n \times m, k, d]$ **rank-metric code** C is a k-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_q^{n\times m}$.
- The **minimum rank distance** of C is $d := \min\{\mathrm{rk}(M) : 0 \neq M \in C\}$.
- For every $M \in C$, $\mathrm{supp}(M) := \mathrm{colsp}(M) \leq \mathbb{F}_q^n$.
- $\mathrm{supp}(C) := \sum_{M\in C} \mathrm{supp}(M)$.
- C is **non-degenerate** if $\mathrm{supp}(C) = E$.
- For every $U \leq E$, $C(U) := \{M \in C \ : \ \mathrm{supp}(M) \leq U^\perp\}$ is called a **shortened subcode** of C.

Rank-Metric Codes

Basic Notions

- An $\mathbb{F}_q$-$[n \times m, k, d]$ **rank-metric code** C is a k-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_q^{n \times m}$.
- The **minimum rank distance** of C is $d := \min\{\mathrm{rk}(M) : 0 \neq M \in C\}$.
- For every $M \in C$, $\mathrm{supp}(M) := \mathrm{colsp}(M) \leq \mathbb{F}_q^n$.
- $\mathrm{supp}(C) := \sum_{M \in C} \mathrm{supp}(M)$.
- C is **non-degenerate** if $\mathrm{supp}(C) = E$.
- For every $U \leq E$, $C(U) := \{M \in C \; : \; \mathrm{supp}(M) \leq U^{\perp}\}$ is called a **shortened subcode** of C.
- **Singleton-like bound:** $k \leq \max\{n, m\}(\min\{n, m\} + d - 1)$.
- Codes attaining the Singleton-like bound are called **MRD**.

Matroids

A **matroid** $\mathcal{M}$ is an ordered pair $([n], r)$ where $r : 2^{[n]} \to \mathbb{Z}$ s.t. $\forall\ A, B \subseteq [n]$

(r1) **(Boundness)** $0 \leq r(A) \leq |A|$.

(r2) **(Monotonicity)** If $A \subseteq B$, then $r(A) \leq r(B)$.

(r3) **(Submodularity)** $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.

Matroids

A **matroid** $\mathcal{M}$ is an ordered pair $([n], r)$ where $r : 2^{[n]} \to \mathbb{Z}$ s.t. $\forall\ A, B \subseteq [n]$

(r1) **(Boundness)** $0 \leq r(A) \leq |A|$.

(r2) **(Monotonicity)** If $A \subseteq B$, then $r(A) \leq r(B)$.

(r3) **(Submodularity)** $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.

Example

Let C be an $[n, k]_q$ code with generator matrix $G := [G^1 | \cdots | G^n]$.

Let $S \subseteq [n]$.

Matroids

A **matroid** $\mathcal{M}$ is an ordered pair $([n], r)$ where $r : 2^{[n]} \to \mathbb{Z}$ s.t. $\forall\ A, B \subseteq [n]$

(r1) **(Boundness)** $0 \leq r(A) \leq |A|$.

(r2) **(Monotonicity)** If $A \subseteq B$, then $r(A) \leq r(B)$.

(r3) **(Submodularity)** $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.

Example

Let C be an $[n, k]_q$ code with generator matrix $G := [G^1 | \cdots | G^n]$.

Let $S \subseteq [n]$. Let C_S : code with generator matrix $[G^s : s \in S]$.

Matroids

A **matroid** $\mathcal{M}$ is an ordered pair $([n], r)$ where $r : 2^{[n]} \to \mathbb{Z}$ s.t. $\forall\ A, B \subseteq [n]$

(r1) **(Boundness)** $0 \leq r(A) \leq |A|$.

(r2) **(Monotonicity)** If $A \subseteq B$, then $r(A) \leq r(B)$.

(r3) **(Submodularity)** $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.

Example

Let C be an $[n, k]_q$ code with generator matrix $G := [G^1 | \cdots | G^n]$.

Let $S \subseteq [n]$. Let C_S : code with generator matrix $[G^s : s \in S]$.

Define $r : 2^{[n]} \to \mathbb{Z}$, $S \mapsto \dim(\langle G^s : s \in S \rangle)$.

Matroids

A **matroid** $\mathcal{M}$ is an ordered pair $([n], r)$ where $r : 2^{[n]} \to \mathbb{Z}$ s.t. $\forall\ A, B \subseteq [n]$

(r1) **(Boundness)** $0 \leq r(A) \leq |A|$.

(r2) **(Monotonicity)** If $A \subseteq B$, then $r(A) \leq r(B)$.

(r3) **(Submodularity)** $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.

Example

Let C be an $[n, k]_q$ code with generator matrix $G := [G^1 | \cdots | G^n]$.

Let $S \subseteq [n]$. Let C_S : code with generator matrix $[G^s : s \in S]$.

Define $r : 2^{[n]} \to \mathbb{Z}, \ \ S \mapsto \dim(\langle G^s : s \in S \rangle)$.

Then $\mathcal{M} = \mathcal{M}[C] := ([n], r)$ is a **representable** matroid.

Matroids from Codes

A **matroid** $\mathcal{M}$ is an ordered pair $([n], r)$ where $r : 2^{[n]} \to \mathbb{Z}$ s.t. $\forall\ A, B \subseteq [n]$

(r1) **(Boundness)** $0 \leq r(A) \leq |A|$.

(r2) **(Monotonicity)** If $A \subseteq B$, then $r(A) \leq r(B)$.

(r3) **(Submodularity)** $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.

Example

Let C be an $[n, k]_q$ code with generator matrix $G := [G^1 | \cdots | G^n]$.

Matroids from Codes

A **matroid** $\mathcal{M}$ is an ordered pair $([n], r)$ where $r : 2^{[n]} \to \mathbb{Z}$ s.t. $\forall\ A, B \subseteq [n]$

(r1) **(Boundness)** $0 \leq r(A) \leq |A|$.

(r2) **(Monotonicity)** If $A \subseteq B$, then $r(A) \leq r(B)$.

(r3) **(Submodularity)** $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.

Example

Let C be an $[n, k]_q$ code with generator matrix $G := [G^1 | \cdots | G^n]$.

Let $S \subseteq [n]$. Let $C_S := \{(c_s \ : \ s \in S) \ : \ c \in C\}$.

Matroids from Codes

A **matroid** $\mathcal{M}$ is an ordered pair $([n], r)$ where $r : 2^{[n]} \to \mathbb{Z}$ s.t. $\forall\ A, B \subseteq [n]$

(r1) **(Boundness)** $0 \leq r(A) \leq |A|$.

(r2) **(Monotonicity)** If $A \subseteq B$, then $r(A) \leq r(B)$.

(r3) **(Submodularity)** $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.

Example

Let C be an $[n, k]_q$ code with generator matrix $G := [G^1 | \cdots | G^n]$.

Let $S \subseteq [n]$. Let $C_S := \{(c_s \ : \ s \in S) \ : \ c \in C\}$.

Define $r : 2^{[n]} \to \mathbb{Z}, \ \ S \mapsto \dim(C_S)$.

Matroids from Codes

A **matroid** $\mathcal{M}$ is an ordered pair $([n], r)$ where $r : 2^{[n]} \to \mathbb{Z}$ s.t. $\forall\ A, B \subseteq [n]$

(r1) **(Boundness)** $0 \leq r(A) \leq |A|$.

(r2) **(Monotonicity)** If $A \subseteq B$, then $r(A) \leq r(B)$.

(r3) **(Submodularity)** $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.

Example

Let C be an $[n, k]_q$ code with generator matrix $G := [G^1 | \cdots | G^n]$.

Let $S \subseteq [n]$. Let $C_S := \{(c_s \ : \ s \in S) \ : \ c \in C\}$.

Define $r : 2^{[n]} \to \mathbb{Z}, \ \ S \mapsto \dim(C_S)$.

Then $\mathcal{M} = \mathcal{M}[C] := ([n], r)$ is a **representable** matroid.

Matroids from Codes

A **matroid** $\mathcal{M}$ is an ordered pair $([n], r)$ where $r : 2^{[n]} \to \mathbb{Z}$ s.t. $\forall\ A, B \subseteq [n]$

(r1) **(Boundness)** $0 \leq r(A) \leq |A|$.

(r2) **(Monotonicity)** If $A \subseteq B$, then $r(A) \leq r(B)$.

(r3) **(Submodularity)** $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.

Example

Let C be an $[n, k]_q$ code with generator matrix $G := [G^1 | \cdots | G^n]$.

Let$S \subseteq [n]$. Let $C(S) := \{c \in C\ :\ c_s = 0 \text{ for all } s \in S\}$,

Matroids from Codes

A **matroid** $\mathcal{M}$ is an ordered pair $([n], r)$ where $r : 2^{[n]} \to \mathbb{Z}$ s.t. $\forall\ A, B \subseteq [n]$

(r1) **(Boundness)** $0 \leq r(A) \leq |A|$.

(r2) **(Monotonicity)** If $A \subseteq B$, then $r(A) \leq r(B)$.

(r3) **(Submodularity)** $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.

Example

Let C be an $[n, k]_q$ code with generator matrix $G := [G^1 | \cdots | G^n]$.

Let$S \subseteq [n]$. Let $C(S) := \{c \in C \ : \ c_s = 0 \text{ for all } s \in S\}$, $C_S \cong C/C(S)$.

Matroids from Codes

A **matroid** $\mathcal{M}$ is an ordered pair $([n], r)$ where $r : 2^{[n]} \to \mathbb{Z}$ s.t. $\forall\ A, B \subseteq [n]$

(r1) **(Boundness)** $0 \leq r(A) \leq |A|$.

(r2) **(Monotonicity)** If $A \subseteq B$, then $r(A) \leq r(B)$.

(r3) **(Submodularity)** $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.

Example

Let C be an $[n, k]_q$ code with generator matrix $G := [G^1|\cdots|G^n]$.

Let$S \subseteq [n]$. Let $C(S) := \{c \in C\ :\ c_s = 0 \text{ for all } s \in S\}$, $C_S \cong C/C(S)$.

Define $r : 2^{[n]} \to \mathbb{Z},\ \ S \mapsto k - \dim(C(S))$.

Matroids from Codes

A **matroid** $\mathcal{M}$ is an ordered pair $([n], r)$ where $r : 2^{[n]} \to \mathbb{Z}$ s.t. $\forall\ A, B \subseteq [n]$

(r1) **(Boundness)** $0 \leq r(A) \leq |A|$.

(r2) **(Monotonicity)** If $A \subseteq B$, then $r(A) \leq r(B)$.

(r3) **(Submodularity)** $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.

Example

Let C be an $[n, k]_q$ code with generator matrix $G := [G^1|\cdots|G^n]$.

Let$S \subseteq [n]$. Let $C(S) := \{c \in C\ :\ c_s = 0 \text{ for all } s \in S\}$, $C_S \cong C/C(S)$.

Define $r : 2^{[n]} \to \mathbb{Z},\ \ S \mapsto k - \dim(C(S))$.

Then $\mathcal{M} = \mathcal{M}[C] := ([n], r)$ is a **representable** matroid.

Matroids from Codes

- C is an $[n, k]_q$ code with generator matrix $G = [G^1 | \cdots | G^n]$.
- $r(S) := \dim(\langle G^s : s \in S \rangle)$, for all $S \subseteq [n]$.

Matroids from Codes

- C is an $[n,k]_q$ code with generator matrix $G = [G^1|\cdots|G^n]$.
- $r(S) := \dim(\langle G^s : s \in S\rangle)$, for all $S \subseteq [n]$.

Example (Extended Hamming Code)

Let C be the $[8,4,4]_2$ code generated by

$$G := \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 & 0 \end{pmatrix}.$$

$$r(S) = \begin{cases} |S| & \text{if } |S| \leq 3 \\ 3 & \text{if } S = \mathrm{supp}(c),\ c \neq (1,1,1,1,1,1,1,1) \\ 4 & \text{otherwise .} \end{cases}$$

Lattices

- A **lattice** $(\mathcal{L}, \leq, \vee, \wedge)$ is a **poset** such that for every $a, b \in \mathcal{L}$, their **join** $a \vee b$ and their **meet** $a \wedge b$ is in $\mathcal{L}$.
- $\mathbf{1}_{\mathcal{L}} = \vee_{a \in \mathcal{L}}$ is the **maximal element** of $\mathcal{L}$.
- $\mathbf{0}_{\mathcal{L}} = \wedge_{a \in \mathcal{L}}$ is the **minimal element** of $\mathcal{L}$.

Lattices

- A **lattice** $(\mathcal{L}, \leq, \vee, \wedge)$ is a **poset** such that for every $a, b \in \mathcal{L}$, their **join** $a \vee b$ and their **meet** $a \wedge b$ is in $\mathcal{L}$.
- $\mathbf{1}_{\mathcal{L}} = \vee_{a \in \mathcal{L}}$ is the **maximal element** of $\mathcal{L}$.
- $\mathbf{0}_{\mathcal{L}} = \wedge_{a \in \mathcal{L}}$ is the **minimal element** of $\mathcal{L}$.
- An **interval** $[a, b] \subseteq \mathcal{L}$ is the set of all $x \in \mathcal{L}$ such that $a \leq x \leq b$.

Lattices

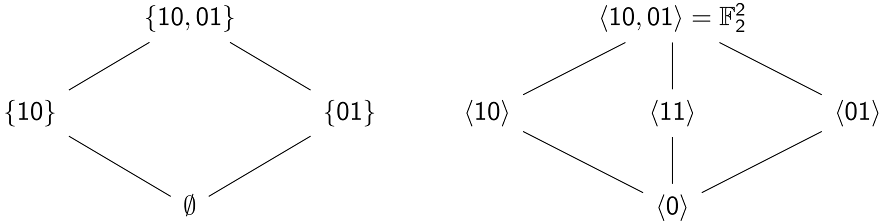
- A **lattice** $(\mathcal{L}, \leq, \vee, \wedge)$ is a **poset** such that for every $a, b \in \mathcal{L}$, their **join** $a \vee b$ and their **meet** $a \wedge b$ is in $\mathcal{L}$.
- $\mathbf{1}_{\mathcal{L}} = \vee_{a \in \mathcal{L}}$ is the **maximal element** of $\mathcal{L}$.
- $\mathbf{0}_{\mathcal{L}} = \wedge_{a \in \mathcal{L}}$ is the **minimal element** of $\mathcal{L}$.
- An **interval** $[a, b] \subseteq \mathcal{L}$ is the set of all $x \in \mathcal{L}$ such that $a \leq x \leq b$.
- Let $c \in [a, b]$. We say that d is a **complement** of c in $[a, b]$ if $c \wedge d = a$ and $c \vee d = b$.
- $\mathcal{L}$ is called **complemented** if every $c \in \mathcal{L}$ has a complement in $\mathcal{L}$.

Lattices

- A **lattice** $(\mathcal{L}, \leq, \vee, \wedge)$ is a **poset** such that for every $a, b \in \mathcal{L}$, their **join** $a \vee b$ and their **meet** $a \wedge b$ is in $\mathcal{L}$.
- $\mathbf{1}_{\mathcal{L}} = \vee_{a \in \mathcal{L}}$ is the **maximal element** of $\mathcal{L}$.
- $\mathbf{0}_{\mathcal{L}} = \wedge_{a \in \mathcal{L}}$ is the **minimal element** of $\mathcal{L}$.
- An **interval** $[a, b] \subseteq \mathcal{L}$ is the set of all $x \in \mathcal{L}$ such that $a \leq x \leq b$.
- Let $c \in [a, b]$. We say that d is a **complement** of c in $[a, b]$ if $c \wedge d = a$ and $c \vee d = b$.
- $\mathcal{L}$ is called **complemented** if every $c \in \mathcal{L}$ has a complement in $\mathcal{L}$.
- A finite **chain** from a to b is a sequence $a = x_1 < \cdots < x_{k+1} = b$ with $x_j \in \mathcal{L}$.
- The **height** of b is the maximum length of all maximal chains from $\mathbf{0}_{\mathcal{L}}$ to b.

Complemented Lattices

Boolean Lattice $(2^{[n]}, \subseteq, \cup, \cap)$	$\longrightarrow$	Subspace Lattice $(\mathcal{L}(E), \leq, +, \cap)$
Matroids	$\longrightarrow$	q-Matroids
Polymatroids	$\longrightarrow$	q-Polymatroids



Matroids $\to$ q-Matroids

Definition

A **matroid** $\mathcal{M}$ is an ordered pair $([n], r)$ where $r : 2^{[n]} \to \mathbb{Z}$ s.t. $\forall\ A, B \subseteq [n]$

(r1) **(Boundness)** $0 \leq r(A) \leq |A|$.

(r2) **(Monotonicity)** If $A \subseteq B$, then $r(A) \leq r(B)$.

(r3) **(Submodularity)** $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.

Matroids $\to$ q-Matroids

Definition

A **matroid** $\mathcal{M}$ is an ordered pair $([n], r)$ where $r : 2^{[n]} \to \mathbb{Z}$ s.t. $\forall\ A, B \subseteq [n]$

(r1) **(Boundness)** $0 \leq r(A) \leq |A|$.

(r2) **(Monotonicity)** If $A \subseteq B$, then $r(A) \leq r(B)$.

(r3) **(Submodularity)** $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$.

Definition (Jurrius, Pellikaan, 2018)

A q-**matroid** is a pair (E, r), $\mathcal{L}(E)$ is the lattice of subspaces of E and $r : \mathcal{L}(E) \to \mathbb{Z}$ is a **rank function** such that $\forall\ A, B \leq E$

(R1) **(Boundness)** $0 \leq r(A) \leq \dim(A)$.

(R2) **(Monotonicity)** If $A \leq B$, then $r(A) \leq r(B)$.

(R3) **(Submodularity)** $r(A + B) + r(A \cap B) \leq r(A) + r(B)$.

R. Jurrius, R. Pellikaan. "Defining the q-analogue of a matroid.", 2018.

Polymatroids $\rightarrow$ q-Polymatroids

Definition

An $(\mathcal{L}, r)$-**(integer) polymatroid** is a pair $\mathcal{M} = (\mathcal{L}, \rho)$ for which $r \in \mathbb{N}_0$ and ρ is a function $\rho : \mathcal{L} \longrightarrow \mathbb{N}_0$ satisfying the following axioms for all $A, B \in \mathcal{L}$.

(R1) **(Boundness)** $0 \leq \rho(A) \leq r \cdot h(A)$.

(R2) **(Monotonicity)** $A \leq B \Rightarrow \rho(A) \leq \rho(B)$.

(R3) **(Submodularity)** $\rho(A \vee B) + \rho(A \wedge B) \leq \rho(A) + \rho(B)$.

Polymatroids $\to$ q-Polymatroids

Definition

An $(\mathcal{L}, r)$-**(integer) polymatroid** is a pair $\mathcal{M} = (\mathcal{L}, \rho)$ for which $r \in \mathbb{N}_0$ and ρ is a function $\rho : \mathcal{L} \longrightarrow \mathbb{N}_0$ satisfying the following axioms for all $A, B \in \mathcal{L}$.

(R1) **(Boundness)** $0 \leq \rho(A) \leq r \cdot h(A)$.

(R2) **(Monotonicity)** $A \leq B \Rightarrow \rho(A) \leq \rho(B)$.

(R3) **(Submodularity)** $\rho(A \vee B) + \rho(A \wedge B) \leq \rho(A) + \rho(B)$.

- $\mathcal{L}$ Boolean lattice:
  - $\mathcal{M}$ is an $(\mathcal{L}, r)$ polymatroid.
  - $r = 1$, $\mathcal{M}$ is a matroid.
- $\mathcal{L} = \mathcal{L}(E)$ Subspace lattice:
  - $\mathcal{M}$ is a (q, r)-**polymatroid** [Gorla+ 2019, Shiromoto 2019].
  - $r = 1$, $\mathcal{M}$ is a q-matroid [Jurrius, Pellikaan 2016].

R. Jurrius, R. Pellikaan. "Defining the q-analogue of a matroid.", 2016.

E. Gorla, R. Jurrius, H. López, A. Ravagnani. "Rank-Metric Codes and q-Polymatroids", 2019.

K. Shiromoto. "Matroids and Codes with the Rank Metric", 2019.

Restriction and Contraction

Let $\mathcal{M} = (\mathcal{L}, \rho)$ be a $(\mathcal{L}, r)$-polymatroid and let $[X, Y]$ be an interval of $\mathcal{L}$.

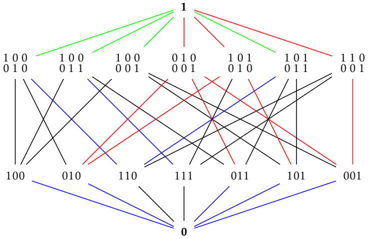
$$\begin{aligned} \rho_{[X,Y]} : \mathcal{L}(E) &\to \mathbb{N}_0 \\ T &\mapsto \rho(T) - \rho(X) \end{aligned}$$

$\mathcal{M}([X, Y]) = ([X, Y], \rho_{[X,Y]})$ is a **minor** of $\mathcal{M}$.

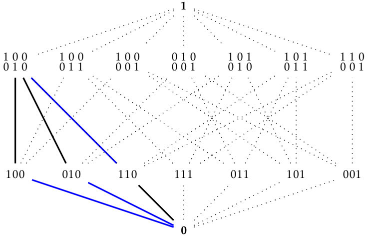
1. We write $\mathcal{M}|_Y := \mathcal{M}([\mathbf{0}, Y])$, which is called the **restriction** of $\mathcal{M}$ to Y.
2. We write $\mathcal{M}/X := \mathcal{M}([X, \mathbf{1}])$, which is called the **contraction** of $\mathcal{M}$ **by** X.

Restriction and Contraction: Example

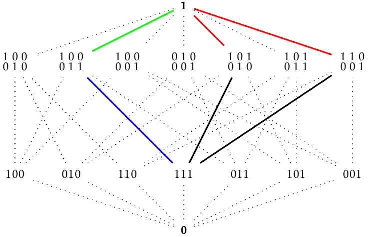
Let $E = \mathbb{F}_2^3$ and $X = \langle(1,1,1)\rangle$, $Y = \langle(1,0,0),(0,1,0)\rangle$.



$\mathcal{M}|_Y$



$\mathcal{M}/X$



Representable q-Polymatroids

Theorem (Gorla+ 2019, Shiromoto 2019)

Let C be an $\mathbb{F}_q$-$[n \times m, k, d]$ rank-metric code. For each subspace $U \leq E$, define

$$C(U) := \{M \in C : \mathrm{supp}(M) \leq U^{\perp}\}.$$

Define

$$\rho : \mathcal{L}(E) \to \mathbb{Z},\ \rho(U) := k - \dim(C(U)).$$

$\mathcal{M}[C] = (E, \rho)$ *is a* (q, m)*-polymatroid.*

- For every $U \leq E$, $\mathcal{M}[C]/U \sim \mathcal{M}[C(U)]$. [Gluesing-Luerssen, Jany, 2022]

E. Gorla, R. Jurrius, H. López, A. Ravagnani. "Rank-Metric Codes and q-Polymatroids", 2019.

K. Shiromoto. "Matroids and Codes with the Rank Metric", 2019.

H. Gluesing-Luerssen, B. Jany, "q-polymatroids and their relation to rank-metric codes, 2022.

Contents

Distinguish Spaces

Definition:

- $U \leq E$.
- $\mathbf{B} = (b_1, \ldots, b_r)$ list of bilinear forms $b_i : \mathbb{F}_q^n \times \mathbb{F}_q^m \to \mathbb{F}_q$.

B distinguishes the space U if

$$\bigcap_{i=1}^{r} \mathrm{lker}(b_i) \leq U^{\perp},$$

where $\mathrm{lker}(b)$ denotes the left kernel of the bilinear form b.

Distinguish Spaces

Definition:

- $U \leq E$.
- $\mathbf{B} = (b_1, \ldots, b_r)$ list of bilinear forms $b_i : \mathbb{F}_q^n \times \mathbb{F}_q^m \to \mathbb{F}_q$.

B distinguishes the space U if

$$\bigcap_{i=1}^{r} \operatorname{lker}(b_i) \leq U^{\perp},$$

where $\operatorname{lker}(b)$ denotes the left kernel of the bilinear form b.

Problem ((q-Analogue of the) Critical Problem)

Find the minimum number c of bilinear forms b_i, such that $(b_1, \ldots, b_c)$ distinguishes a fixed space $U \leq E$.

Distinguish Spaces

Problem ((*q*-Analogue of the) Critical Problem)

Let C be an $\mathbb{F}_q$-$[n \times m, k]$ rank-metric codes. Let $U \leq E$. Find the minimum number c of codewords M_i of C, such that

$$\sum_{i=1}^{c} \mathrm{supp}(M_i) = U.$$

Distinguish Spaces

Problem ((*q*-Analogue of the) Critical Problem)

Let C be an $\mathbb{F}_q$-$[n \times m, k]$ rank-metric codes. Let $U \leq E$. Find the minimum number c of codewords M_i of C, such that

$$\sum_{i=1}^{c} \mathrm{supp}(M_i) = U.$$

Definition: the Critical Exponent of C

$\mathrm{crit}(C)$: least number t of codewords of C, whose supports span $\mathrm{supp}(C)$.

Distinguish Spaces

Problem ((*q*-Analogue of the) Critical Problem)

Let C be an $\mathbb{F}_q$-$[n \times m, k]$ rank-metric codes. Let $U \leq E$. Find the minimum number c of codewords M_i of C, such that

$$\sum_{i=1}^{c} \mathrm{supp}(M_i) = U.$$

Definition: the Critical Exponent of C

$\mathrm{crit}(\mathcal{M}[C])$: least number t of codewords of C, whose supports span $\mathrm{supp}(C)$.

Möbius Function on a Poset

Let $(P, \leq)$ be a partially ordered set. The Möbius Function on P is defined by

$$\mu(x,y) := \begin{cases} 1 & \text{if } x = y, \\ -\sum_{x \leq z < y} \mu(x,z) & \text{if } x < y, \\ 0 & \text{otherwise.} \end{cases}$$

Lemma (Möbius Inversion formula)

Let $f, g : P \to \mathbb{Z}$ be two functions on a poset P. Then

1. $f(x) = \sum_{x \leq y} g(y)$ *if and only if* $g(x) = \sum_{x \leq y} \mu(x,y) f(y)$.
2. $f(x) = \sum_{x \geq y} g(y)$ *if and only if* $g(x) = \sum_{x \geq y} \mu(y,x) f(y)$.

$\mathcal{L}$	Boolean lattice	Subspace lattice
$\mu(0, U)$	$(-1)^{\|U\|}$	$(-1)^{\dim(U)} q^{\binom{\dim(U)}{2}}$

The Characteristic Polynomial

Let $\mathcal{M} = (E, \rho)$ be a q-polymatroid.

Definition: The **characteristic polynomial** of $\mathcal{M}$ is the polynomial in $\mathbb{Z}[z]$ defined by

$$p(\mathcal{M}; z) := \sum_{0 \leq A \leq E} \mu(0, A) z^{\rho(E) - \rho(A)}.$$

The Characteristic Polynomial

Let $\mathcal{M} = (E, \rho)$ be a q-polymatroid.

Definition: The **characteristic polynomial** of $\mathcal{M}$ is the polynomial in $\mathbb{Z}[z]$ defined by

$$p(\mathcal{M}; z) := \sum_{0 \leq A \leq E} \mu(0, A) z^{\rho(E) - \rho(A)}.$$

Properties:

- $p(\mathcal{M}/U; z) = \sum_{U \leq A \leq E} \mu(U, A) z^{\rho(E) - \rho(A)}$.

The Characteristic Polynomial

Let $\mathcal{M} = (E, \rho)$ be a q-polymatroid.

Definition: The **characteristic polynomial** of $\mathcal{M}$ is the polynomial in $\mathbb{Z}[z]$ defined by

$$p(\mathcal{M}; z) := \sum_{0 \leq A \leq E} \mu(0, A) z^{\rho(E) - \rho(A)}.$$

Properties:

- $p(\mathcal{M}/U; z) = \sum_{U \leq A \leq E} \mu(U, A) z^{\rho(E) - \rho(A)}$.
- $z^{\rho(E) - \rho(U)} = \sum_{U \leq A \leq E} p(\mathcal{M}/A; z)$ (**by Möbius Inversion**).

The Characteristic Polynomial

Let $\mathcal{M} = (E, \rho)$ be a q-polymatroid.

Definition: The **characteristic polynomial** of $\mathcal{M}$ is the polynomial in $\mathbb{Z}[z]$ defined by

$$p(\mathcal{M}; z) := \sum_{0 \leq A \leq E} \mu(0, A) z^{\rho(E) - \rho(A)}.$$

Properties:

- $p(\mathcal{M}/U; z) = \sum_{U \leq A \leq E} \mu(U, A) z^{\rho(E) - \rho(A)}$.
- $z^{\rho(E) - \rho(U)} = \sum_{U \leq A \leq E} p(\mathcal{M}/A; z)$ (**by Möbius Inversion**).
- If $\mathcal{M} = \mathcal{M}[C]$ then $|C(U)| = \sum_{U \leq A \leq E} p(\mathcal{M}/A; q)$.

The Critical Theorem for q-Polymatroids

- $p(\mathcal{M}/U;z) = \sum_{U \leq A \leq E} \mu(U,A) z^{\rho(E)-\rho(A)}$.

Theorem (A., Byrne (2022))

Let C be an $\mathbb{F}_q$-$[n \times m, k]$ rank-metric code, $\mathcal{M} = \mathcal{M}[C]$ and let $U \leq E$.

$$|\{(X_1,\ldots,X_t) \ : \ X_i \in C, \mathrm{supp}(X_1) + \cdots + \mathrm{supp}(X_t) = U\}| = p(\mathcal{M}/U^{\perp}; q^t).$$

The Critical Theorem for q-Polymatroids

- $p(\mathcal{M}/U; z) = \sum_{U \leq A \leq E} \mu(U, A) z^{\rho(E)-\rho(A)}$.

Theorem (A., Byrne (2022))

Let C be an $\mathbb{F}_q$-$[n \times m, k]$ rank-metric code, $\mathcal{M} = \mathcal{M}[C]$ and let $U \leq E$.

$$|\{(X_1, \dots, X_t) \ : \ X_i \in C, \mathrm{supp}(X_1) + \cdots + \mathrm{supp}(X_t) = U\}| = p(\mathcal{M}/U^{\perp}; q^t).$$

Proof:

$$f(W) := |\{(X_1, \dots, X_t) \in C^t : \sum_{i=1}^{t} \mathrm{colsp}(X_i) = W^{\perp}\}|,$$

$$g(W) := |\{(X_1, \dots, X_t) \in C^t : \sum_{i=1}^{t} \mathrm{colsp}(X_i) \leq W^{\perp}\}|.$$

The Critical Theorem for q-Polymatroids

- $p(\mathcal{M}/U;z) = \sum_{U \leq A \leq E} \mu(U,A) z^{\rho(E)-\rho(A)}$.

Theorem (A., Byrne (2022))

Let C be an $\mathbb{F}_q$-$[n \times m, k]$ rank-metric code, $\mathcal{M} = \mathcal{M}[C]$ and let $U \leq E$.

$$|\{(X_1,\dots,X_t) \ : \ X_i \in C, \mathrm{supp}(X_1) + \cdots + \mathrm{supp}(X_t) = U\}| = p(\mathcal{M}/U^\perp; q^t).$$

Proof:

$$f(W) := |\{(X_1,\dots,X_t) \in C^t : \sum_{i=1}^{t} \mathrm{colsp}(X_i) = W^\perp\}|,$$

$$g(W) := |\{(X_1,\dots,X_t) \in C^t : \sum_{i=1}^{t} \mathrm{colsp}(X_i) \leq W^\perp\}|.$$

$$g(W) = \sum_{V \in [W,E]} f(V).$$

$$g(W) = |\{(X_1,\dots,X_t) \in C^t : \mathrm{colsp}(X_i) \leq W^\perp \ \forall\, i \in [t]\}| = |C(W)|^t.$$

The Critical Theorem for q-Polymatroids

- $p(\mathcal{M}/U; z) = \sum_{U \leq A \leq E} \mu(U, A) z^{\rho(E)-\rho(A)}$.

Theorem (A., Byrne (2022))

Let C be an $\mathbb{F}_q$-$[n \times m, k]$ rank-metric code, $\mathcal{M} = \mathcal{M}[C]$ and let $U \leq E$.

$$|\{(X_1, \dots, X_t) \ : \ X_i \in C, \mathrm{supp}(X_1) + \dots + \mathrm{supp}(X_t) = U\}| = p(\mathcal{M}/U^{\perp}; q^t).$$

Proof:

$$f(W) := |\{(X_1, \dots, X_t) \in C^t : \sum_{i=1}^{t} \mathrm{colsp}(X_i) = W^{\perp}\}|,$$

$$g(W) := |\{(X_1, \dots, X_t) \in C^t : \sum_{i=1}^{t} \mathrm{colsp}(X_i) \leq W^{\perp}\}|.$$

$$g(W) = \sum_{V \in [W,E]} f(V).$$

$$g(W) = |\{(X_1, \dots, X_t) \in C^t : \mathrm{colsp}(X_i) \leq W^{\perp} \ \forall \ i \in [t]\}| = |C(W)|^t.$$

$$f(W) = \sum_{V \in [W,E]} \mu(W, V) g(V) = \sum_{V \in [W,E]} \mu(W, V) |C(V)|^t = \sum_{V \in [W,E]} \mu(W, V) q^{t(k-\rho(V))} = P(\mathcal{M}/W; q^t).$$

G. Alfarano, E. Byrne. "The Critical Theorem for q-Polymatroids.", 2023.

Critical Exponent

Corollary

If C is a non-degenerate $\mathbb{F}_q$-$[n \times m, k]$ code, then

$$|\{(X_1, \dots, X_t) \ : \ X_i \in C, \mathrm{supp}(X_1) + \dots + \mathrm{supp}(X_t) = \mathbb{F}_q^n\}| = p(\mathcal{M}; q^t).$$

Critical Exponent

Corollary

If C is a non-degenerate $\mathbb{F}_q$-$[n \times m, k]$ code, then

$$|\{(X_1, \ldots, X_t) \; : \; X_i \in C, \mathrm{supp}(X_1) + \cdots + \mathrm{supp}(X_t) = \mathbb{F}_q^n\}| = p(\mathcal{M}; q^t).$$

$$\mathrm{crit}(\mathcal{M}[C]) = \begin{cases} \infty & \text{if } C \text{ is degenerate,} \\ \min\{r : p(\mathcal{M}; q^r) > 0\} & \text{otherwise.} \end{cases}$$

- Ben Jany (2022) gave an alternative proof for the q-matroid case.
- Imamura and Shiromoto, independently showed a similar result (2023).

Example

Let C be the $\mathbb{F}_2$-$[5 \times 3, 6, 1]$ rank-metric code generated by the matrices

$$\begin{pmatrix}1&0&0\\0&0&0\\0&0&0\\0&0&0\\0&0&0\end{pmatrix}, \begin{pmatrix}0&0&0\\0&1&0\\0&0&0\\0&0&0\\0&0&0\end{pmatrix}, \begin{pmatrix}0&0&0\\0&0&0\\0&0&1\\0&0&1\\0&0&0\end{pmatrix}, \begin{pmatrix}0&1&0\\0&1&1\\0&0&0\\0&0&1\\1&0&1\end{pmatrix}, \begin{pmatrix}0&1&1\\1&0&1\\1&0&1\\1&1&1\\0&1&0\end{pmatrix}, \begin{pmatrix}0&1&1\\1&1&1\\1&1&1\\0&1&0\\1&0&0\end{pmatrix}.$$

Let $\mathcal{M} = (\mathbb{F}_2^5, \rho)$ be the $(q, 3)$-polymatroid induced by C. We calculate the characteristic polynomial of $\mathcal{M}$,

$$p(\mathcal{M}; z) := \sum_{X \leq \mathbb{F}_2^5} \mu(0, X) z^{\rho(\mathbb{F}_2^5) - \rho(X)} = \cdots = z^6 - 4z^4 - 25z^3 + 44z^2 + 40z - 56.$$

- $p(\mathcal{M}; 1) = p(\mathcal{M}; 2) = 0.$
- $p(\mathcal{M}; 2^2) = 2280 > 0.$

Hence $\mathrm{crit}(\mathcal{M}) = 2$. Indeed

$$X_1 = \begin{pmatrix}0&1&0\\0&1&1\\0&0&0\\0&0&1\\1&0&1\end{pmatrix} \quad \text{and} \quad X_2 = \begin{pmatrix}0&1&1\\1&1&1\\1&1&1\\0&1&0\\1&0&0\end{pmatrix}.$$

First Bound

Proposition

Let C be a non-degenerate $\mathbb{F}_q$-$[n \times m, k]$ code and let $\mathcal{M} = \mathcal{M}[C]$ be the q-polymatroid associated to C. Then

$$\left\lceil \frac{n}{m} \right\rceil \leq \mathrm{crit}(\mathcal{M}) \leq k.$$

First Bound

Proposition

Let C be a non-degenerate $\mathbb{F}_q$-$[n \times m, k]$ code and let $\mathcal{M} = \mathcal{M}[C]$ be the q-polymatroid associated to C. Then

$$\left\lceil \frac{n}{m} \right\rceil \leq \mathrm{crit}(\mathcal{M}) \leq k.$$

Proof.

If $\mathrm{crit}(\mathcal{M}) = t$, then there are $X_1, \ldots, X_t \in C$ such that

$$\sum_{i=1}^{t} \mathrm{supp}(X_i) = \mathbb{F}_q^n.$$

Then,

$$n = \dim_{\mathbb{F}_q} \left(\sum_{i=1}^{t} \mathrm{supp}(X_i) \right) \leq mt.$$

□

Rank-Metric Codes Linear over $\mathbb{F}_{q^m}$

- $\mathbb{F}_{q^m}/\mathbb{F}_q$ finite extension field
- k, n positive integers, with $k \leq n$

Definition

An $[n,k]_{q^m/q}$ **rank-metric code** is an $\mathbb{F}_{q^m}$-linear subspace $C \leq \mathbb{F}_{q^m}^n$.

- n is the **length** of C.
- k is the **dimension** of C.

Let $v \in \mathbb{F}_{q^m}^n$ and fix a basis $\Gamma = \{\gamma_1, \ldots, \gamma_m\}$ of $\mathbb{F}_{q^m}/\mathbb{F}_q$. Let $\Gamma(v) \in \mathbb{F}_q^{m \times n}$ be the matrix defined by

$$v_j = \sum_{i=1}^{m} \Gamma(v)_{ij} \gamma_i.$$

Definition

The Γ-**support** of a vector $v \in \mathbb{F}_{q^m}^n$ is the rowspace of $\Gamma(v)$. It is denoted by $\sigma_\Gamma(v) \subseteq \mathbb{F}_q^n$.

Rank-Metric Codes

- $\mathbb{F}_{q^m}/\mathbb{F}_q$ finite extension field
- k, n positive integers, with $k \leq n$

Definition

An $[n, k]_{q^m/q}$ **rank-metric code** is an $\mathbb{F}_{q^m}$-linear subspace $C \leq \mathbb{F}_{q^m}^n$.

- n is the **length** of C.
- k is the **dimension** of C.

- For any $v \in \mathbb{F}_{q^m}^n$, $\sigma(v) = \mathrm{rowsp}(\Gamma(v)) \leq \mathbb{F}_q^n$.
- The **rank weight** of $v \in \mathbb{F}_{q^m}^n$ is $\mathrm{rk}(v) = \dim_{\mathbb{F}_q}(\sigma(v))$.
- C possesses a **generator matrix** $G \in \mathbb{F}_{q^m}^{k \times n}$:

$$C = \{vG \mid v \in \mathbb{F}_{q^m}^k\},$$

  i.e. the rows of G form a **basis** of C.

- C is **non-degenerate** if the columns of G are $\mathbb{F}_q$-independent.

The Geometry of Rank-Metric Codes (q-systems)

Consider an $[n, k]_{q^m/q}$ non-degenerate rank-metric code C with generator matrix $G = (g_{i,j})$. A basis for C is given by the rows of G.

$$\begin{matrix} \rightarrow \\ \rightarrow \\ \\ \rightarrow \end{matrix} \begin{pmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,n} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,n} \\ \vdots & \vdots & & \vdots \\ g_{k,1} & g_{k,2} & \cdots & g_{k,n} \end{pmatrix}$$

The Geometry of Rank-Metric Codes (q-systems)

We can instead consider the columns of G.

$$\begin{matrix} \downarrow & \downarrow & & \downarrow \end{matrix}$$
$$\begin{pmatrix} g_{1,1} & g_{1,2} & \cdots & g_{1,n} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,n} \\ \vdots & \vdots & & \vdots \\ g_{k,1} & g_{k,2} & \cdots & g_{k,n} \end{pmatrix}$$

The Geometry of Rank-Metric Codes (q-systems)

We can instead consider the $\mathbb{F}_q$-span $\mathcal{U}$ of the columns of G.

$$\left\langle \begin{matrix} \downarrow & \downarrow & & \downarrow \\ g_{1,1} & g_{1,2} & \cdots & g_{1,n} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,n} \\ \vdots & \vdots & & \vdots \\ g_{k,1} & g_{k,2} & \cdots & g_{k,n} \end{matrix} \right\rangle_{\mathbb{F}_q}$$

The Geometry of Rank-Metric Codes (q-systems)

We can instead consider the $\mathbb{F}_q$-span $\mathcal{U}$ of the columns of G.

$$\left\langle \begin{matrix} \downarrow & \downarrow & & \downarrow \\ g_{1,1} & g_{1,2} & \cdots & g_{1,n} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,n} \\ \vdots & \vdots & & \vdots \\ g_{k,1} & g_{k,2} & \cdots & g_{k,n} \end{matrix} \right\rangle_{\mathbb{F}_q}$$

Definition

$\mathcal{U}$ is called $[n,k]_{q^m/q}$ **system** associated to G.

The Geometry of Rank-Metric Codes (q-systems)

We can instead consider the $\mathbb{F}_q$-span $\mathcal{U}$ of the columns of G.

$$\left\langle \begin{matrix} \downarrow & \downarrow & & \downarrow \\ g_{1,1} & g_{1,2} & \cdots & g_{1,n} \\ g_{2,1} & g_{2,2} & \cdots & g_{2,n} \\ \vdots & \vdots & & \vdots \\ g_{k,1} & g_{k,2} & \cdots & g_{k,n} \end{matrix} \right\rangle_{\mathbb{F}_q}$$

Definition

$\mathcal{U}$ is called $[n, k]_{q^m/q}$ **system** associated to G.

Corollary

Let $\mathcal{M}$ be the q-matroid induced by C. Then

$$\mathrm{crit}(\mathcal{M}) = \min\{r \in \mathbb{N} \mid \exists\ \mathbb{F}_{q^m}\text{-hyperplanes } H_1, \ldots, H_r \text{ such that } \mathcal{U} \cap H_1 \cap \ldots \cap H_r = 0\}.$$

Critical Problem for $\mathbb{F}_{q^m}$-Linear Codes

Lemma (A., Borello, Neri, Ravagnani 2022)

A non-degenerate $[n, k]_{q^m/q}$ code contains a codeword of rank equal to $\min\{m, n\}$.

Critical Problem for $\mathbb{F}_{q^m}$-Linear Codes

Lemma (A., Borello, Neri, Ravagnani 2022)

A non-degenerate $[n,k]_{q^m/q}$ *code contains a codeword of rank equal to* $\min\{m,n\}$.

Theorem (A., Byrne 2023)

Let $\mathcal{M} = \mathcal{M}[C]$. *Then* $\mathrm{crit}(\mathcal{M}) = \left\lceil \frac{n}{m} \right\rceil$.

Critical Problem for $\mathbb{F}_{q^m}$-Linear Codes

Lemma (A., Borello, Neri, Ravagnani 2022)

A non-degenerate $[n,k]_{q^m/q}$ code contains a codeword of rank equal to $\min\{m,n\}$.

Theorem (A., Byrne 2023)

Let $\mathcal{M} = \mathcal{M}[C]$. Then $\mathrm{crit}(\mathcal{M}) = \left\lceil \frac{n}{m} \right\rceil$.

Sketch of the Proof:

- Write $n = am + b$, with $a, b \in \mathbb{N}_0$ and $0 \leq b < m$.

Critical Problem for $\mathbb{F}_{q^m}$-Linear Codes

Lemma (A., Borello, Neri, Ravagnani 2022)

A non-degenerate $[n,k]_{q^m/q}$ code contains a codeword of rank equal to $\min\{m,n\}$.

Theorem (A., Byrne 2023)

Let $\mathcal{M} = \mathcal{M}[C]$. Then $\mathrm{crit}(\mathcal{M}) = \left\lceil \frac{n}{m} \right\rceil$.

Sketch of the Proof:

- Write $n = am + b$, with $a, b \in \mathbb{N}_0$ and $0 \leq b < m$.
- If $a = 0$, then $n < m$. By Lemma $\mathrm{crit}(\mathcal{M}) = 1 = \left\lceil \frac{n}{m} \right\rceil$.

Critical Problem for $\mathbb{F}_{q^m}$-Linear Codes

Lemma (A., Borello, Neri, Ravagnani 2022)

A non-degenerate $[n,k]_{q^m/q}$ *code contains a codeword of rank equal to* $\min\{m,n\}$.

Theorem (A., Byrne 2023)

Let $\mathcal{M} = \mathcal{M}[C]$. *Then* $\mathrm{crit}(\mathcal{M}) = \left\lceil \frac{n}{m} \right\rceil$.

Sketch of the Proof:

- Write $n = am + b$, with $a, b \in \mathbb{N}_0$ and $0 \leq b < m$.
- If $a = 0$, then $n < m$. By Lemma $\mathrm{crit}(\mathcal{M}) = 1 = \left\lceil \frac{n}{m} \right\rceil$.
- Assume that an $[n', k]_{q^m/q}$ non-degenerate code s.t. $n' = a'm + b'$, with $a' < a$, has critical exponent $\left\lceil \frac{n'}{m} \right\rceil$.

Critical Problem for $\mathbb{F}_{q^m}$-Linear Codes

Lemma (A., Borello, Neri, Ravagnani 2022)

A non-degenerate $[n,k]_{q^m/q}$ code contains a codeword of rank equal to $\min\{m,n\}$.

Theorem (A., Byrne 2023)

Let $\mathcal{M} = \mathcal{M}[C]$*. Then* $\mathrm{crit}(\mathcal{M}) = \left\lceil \frac{n}{m} \right\rceil$.

Sketch of the Proof:

- Write $n = am + b$, with $a, b \in \mathbb{N}_0$ and $0 \leq b < m$.
- If $a = 0$, then $n < m$. By Lemma $\mathrm{crit}(\mathcal{M}) = 1 = \left\lceil \frac{n}{m} \right\rceil$.
- Assume that an $[n', k]_{q^m/q}$ non-degenerate code s.t. $n' = a'm + b'$, with $a' < a$, has critical exponent $\left\lceil \frac{n'}{m} \right\rceil$.
- There exists a codeword $c = (x_1, \dots, x_m, 0, \dots, 0)$, with rank equal to m.

Critical Problem for $\mathbb{F}_{q^m}$-Linear Codes

Lemma (A., Borello, Neri, Ravagnani 2022)

A non-degenerate $[n, k]_{q^m/q}$ code contains a codeword of rank equal to $\min\{m, n\}$.

Theorem (A., Byrne 2023)

Let $\mathcal{M} = \mathcal{M}[C]$. *Then* $\mathrm{crit}(\mathcal{M}) = \left\lceil \frac{n}{m} \right\rceil$.

Sketch of the Proof:

- Write $n = am + b$, with $a, b \in \mathbb{N}_0$ and $0 \leq b < m$.
- If $a = 0$, then $n < m$. By Lemma $\mathrm{crit}(\mathcal{M}) = 1 = \left\lceil \frac{n}{m} \right\rceil$.
- Assume that an $[n', k]_{q^m/q}$ non-degenerate code s.t. $n' = a'm + b'$, with $a' < a$, has critical exponent $\left\lceil \frac{n'}{m} \right\rceil$.
- There exists a codeword $c = (x_1, \ldots, x_m, 0, \ldots, 0)$, with rank equal to m.
- Construct $C_1 =\leq \mathbb{F}_{q^m}^{n-m}$. Since $n' = n - m = (a-1)m + b$, by the induction hypothesis, the critical exponent of $\mathcal{M}[C_1]$ is $\left\lceil \frac{n-m}{m} \right\rceil$.

Critical Problem for $\mathbb{F}_{q^m}$-Linear Codes

Lemma (A., Borello, Neri, Ravagnani 2022)

A non-degenerate $[n,k]_{q^m/q}$ code contains a codeword of rank equal to $\min\{m,n\}$.

Theorem (A., Byrne 2023)

Let $\mathcal{M}=\mathcal{M}[C]$. *Then* $\mathrm{crit}(\mathcal{M})=\left\lceil \frac{n}{m} \right\rceil$.

Sketch of the Proof:

- Write $n=am+b$, with $a,b\in\mathbb{N}_0$ and $0\leq b<m$.
- If $a=0$, then $n<m$. By Lemma $\mathrm{crit}(\mathcal{M})=1=\left\lceil \frac{n}{m} \right\rceil$.
- Assume that an $[n',k]_{q^m/q}$ non-degenerate code s.t. $n'=a'm+b'$, with $a'<a$, has critical exponent $\left\lceil \frac{n'}{m} \right\rceil$.
- There exists a codeword $c=(x_1,\ldots,x_m,0,\ldots,0)$, with rank equal to m.
- Construct $C_1 =\leq \mathbb{F}_{q^m}^{n-m}$. Since $n'=n-m=(a-1)m+b$, by the induction hypothesis, the critical exponent of $\mathcal{M}[C_1]$ is $\left\lceil \frac{n-m}{m} \right\rceil$.
- Observe that these words are now enough to show the full result.

Critical Problem for $\mathbb{F}_{q^m}$-Linear Codes

Lemma (A., Borello, Neri, Ravagnani 2022)

A non-degenerate $[n,k]_{q^m/q}$ *code contains a codeword of rank equal to* $\min\{m,n\}$.

Theorem (A., Byrne 2023)

Let $\mathcal{M} = \mathcal{M}[C]$. *Then* $\mathrm{crit}(\mathcal{M}) = \left\lceil \frac{n}{m} \right\rceil$.

Sketch of the Proof:

- Write $n = am + b$, with $a, b \in \mathbb{N}_0$ and $0 \leq b < m$.
- If $a = 0$, then $n < m$. By Lemma $\mathrm{crit}(\mathcal{M}) = 1 = \left\lceil \frac{n}{m} \right\rceil$.
- Assume that an $[n', k]_{q^m/q}$ non-degenerate code s.t. $n' = a'm + b'$, with $a' < a$, has critical exponent $\left\lceil \frac{n'}{m} \right\rceil$.
- There exists a codeword $c = (x_1, \ldots, x_m, 0, \ldots, 0)$, with rank equal to m.
- Construct $C_1 = \leq \mathbb{F}_{q^m}^{n-m}$. Since $n' = n - m = (a-1)m + b$, by the induction hypothesis, the critical exponent of $\mathcal{M}[C_1]$ is $\left\lceil \frac{n-m}{m} \right\rceil$.
- Observe that these words are now enough to show the full result.

O. Polverino, P. Santonastaso, J. Sheekey, F. Zullo. "Divisible linear rank metric codes.", 2023.

The General Case

- If C is non-degenerate and $\mathbb{F}_{q^m}$-linear then $\mathrm{crit}(C) = \left\lceil \frac{n}{m} \right\rceil$.

The General Case

- If C is non-degenerate and $\mathbb{F}_{q^m}$-linear then $\mathrm{crit}(C) = \left\lceil \frac{n}{m} \right\rceil$.

Are there other "families" of codes for which we can compute the critical exponent?

The General Case

- If C is non-degenerate and $\mathbb{F}_{q^m}$-linear then $\mathrm{crit}(C) = \left\lceil \frac{n}{m} \right\rceil$.

Are there other "families" of codes for which we can compute the critical exponent?

What about MRD codes?

The General Case

- If C is non-degenerate and $\mathbb{F}_{q^m}$-linear then $\mathrm{crit}(C) = \left\lceil \frac{n}{m} \right\rceil$.

Are there other "families" of codes for which we can compute the critical exponent?

What about MRD codes?

Let C be an $\mathbb{F}_q$-$[n \times m, k, d]$ MRD code.

The General Case

- If C is non-degenerate and $\mathbb{F}_{q^m}$-linear then $\mathrm{crit}(C) = \left\lceil \frac{n}{m} \right\rceil$.

Are there other "families" of codes for which we can compute the critical exponent?

What about MRD codes?

Let C be an $\mathbb{F}_q$-$[n \times m, k, d]$ MRD code.

1. If C is $\mathbb{F}_{q^m}$-linear then $\mathrm{crit}(C) = \left\lceil \frac{n}{m} \right\rceil$.

The General Case

- If C is non-degenerate and $\mathbb{F}_{q^m}$-linear then $\mathrm{crit}(C) = \lceil \frac{n}{m} \rceil$.

Are there other "families" of codes for which we can compute the critical exponent?

What about MRD codes?

Let C be an $\mathbb{F}_q$-$[n \times m, k, d]$ MRD code.

1. If C is $\mathbb{F}_{q^m}$-linear then $\mathrm{crit}(C) = \lceil \frac{n}{m} \rceil$.
2. $n \leq m$, then $\mathrm{crit}(C) = \lceil \frac{n}{m} \rceil$.

The General Case

- If C is non-degenerate and $\mathbb{F}_{q^m}$-linear then $\mathrm{crit}(C) = \lceil \frac{n}{m} \rceil$.

Are there other “families” of codes for which we can compute the critical exponent?

What about MRD codes?

Let C be an $\mathbb{F}_q$-$[n \times m, k, d]$ MRD code.

1. If C is $\mathbb{F}_{q^m}$-linear then $\mathrm{crit}(C) = \lceil \frac{n}{m} \rceil$.
2. $n \leq m$, then $\mathrm{crit}(C) = \lceil \frac{n}{m} \rceil$.
3. $m < n \leq 2m - d$, then $\mathrm{crit}(C) = \lceil \frac{n}{m} \rceil$.

The General Case

- If C is non-degenerate and $\mathbb{F}_{q^m}$-linear then $\mathrm{crit}(C) = \lceil \frac{n}{m} \rceil$.

Are there other "families" of codes for which we can compute the critical exponent?

What about MRD codes?

Let C be an $\mathbb{F}_q$-$[n \times m, k, d]$ MRD code.

1. If C is $\mathbb{F}_{q^m}$-linear then $\mathrm{crit}(C) = \lceil \frac{n}{m} \rceil$.
2. $n \leq m$, then $\mathrm{crit}(C) = \lceil \frac{n}{m} \rceil$.
3. $m < n \leq 2m - d$, then $\mathrm{crit}(C) = \lceil \frac{n}{m} \rceil$.
4. $m = n - 1$, $d = n - 1$, then $\mathrm{crit}(C) = \lceil \frac{n}{m} \rceil$.

The General Case

- If C is non-degenerate and $\mathbb{F}_{q^m}$-linear then $\mathrm{crit}(C) = \lceil \frac{n}{m} \rceil$.

Are there other "families" of codes for which we can compute the critical exponent?

What about MRD codes?

Let C be an $\mathbb{F}_q$-$[n \times m, k, d]$ MRD code.

1. If C is $\mathbb{F}_{q^m}$-linear then $\mathrm{crit}(C) = \lceil \frac{n}{m} \rceil$.
2. $n \leq m$, then $\mathrm{crit}(C) = \lceil \frac{n}{m} \rceil$.
3. $m < n \leq 2m - d$, then $\mathrm{crit}(C) = \lceil \frac{n}{m} \rceil$.
4. $m = n - 1$, $d = n - 1$, then $\mathrm{crit}(C) = \lceil \frac{n}{m} \rceil$.

What about the other cases?

Thank you for the attention!

Grazie per l'attenzione!