Rank Metric Code Invariants : A q-polymatroid approach

ACT21

Benjamin Jany

June 10, 2021

Outline

Intro

- There has been a recent focus on studying linear network coding. The appropriate Mathematical object for this are rank metric codes.
- Code invariants are useful to determine the quality of a code, such as its error-correction capability or its security performance.
- How can we extract these useful invariants from the codes?

Rank Metric Codes

Rank Metric Codes

Definition

- The rank metric on $\mathbb{F}_q^{n\times m}$ is,

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

- A Rank Metric Code, is a subspace $\mathcal{C}$ of the metric space $(\mathbb{F}_q^{n\times m}, d)$, where d is the rank metric.
- Let $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ be a rank metric code, the rank distance of $\mathcal{C}$ is

$$d(\mathcal{C}) := \min_{M\in\mathcal{C}\setminus 0} d(M,0) = \min_{M\in\mathcal{C}\setminus 0} \mathrm{rk}(M).$$

Singleton Bound

Theorem (Singleton Bound)

Let $\mathcal{C} \subseteq \mathbb{F}_q^{n \times m}$ be a rank metric code with rank distance d. Let $\dim \mathcal{C} = k$ then

$$k \leq \max\{n, m\}(\min\{n, m\} - d + 1)$$

If equality holds $\mathcal{C}$ is said to be a Maximum Rank Distance (MRD) code.

Example

Let $\mathcal{C} \subseteq \mathbb{F}_2^{3\times 4}$, where

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

Note $\dim \mathcal{C} = 4$, hence from the Singleton Bound: $4 \leq 4(3 - d + 1)$, i.e. $d \leq 3$.

Furthermore one can check that $d(\mathcal{C}) = 3$. Hence $\mathcal{C}$ is an MRD code.

Code Invariant

Definition

- Two rank metric codes $\mathcal{C}_1, \mathcal{C}_2 \subseteq \mathbb{F}_q^{n \times m}$ are equivalent if there exist an isometry $\psi : \mathbb{F}_q^{n \times m} \to \mathbb{F}_q^{n \times m}$ such that $\psi(\mathcal{C}_1) = \mathcal{C}_2$.
- A code invariant is a "property" of a rank metric code that is preserved under code equivalence.

Example

Examples of Code Invariants:

a) Rank distance

b) Generalized weights

c) Rank Weight enumerator

Generalized Weights

Let $m \geq n$.

Definition (Ravagnani, 2014)

$A \subseteq \mathbb{F}_q^{n \times m}$ is an anticode if

$$\dim A = m \max_{M \in A} \{\mathrm{rk}(M)\}.$$

Let $\mathcal{A}_q(n, m)$ be the collection of anticodes of $\mathbb{F}_q^{n \times m}$.

Definition (Ravagnani, 2014)

Let $\mathcal{C} \subseteq \mathbb{F}_q^{n \times m}$ be a rank metric code. The r-th generalized weight of $\mathcal{C}$ is

$$d_r(\mathcal{C}) = \frac{1}{m} \min\{\dim A \mid A \in \mathcal{A}_q(n, m), \dim(A \cap \mathcal{C}) \geq r\}.$$

q-Polymatroids

q-Polymatroid

$\mathcal{V}(\mathbb{F}_q^n) := \{\text{all subspaces of } \mathbb{F}_q^n\}$

Definition (Gorla, Jurrius, López, Ravagnani, 2019)

Let $\rho : \mathcal{V}(\mathbb{F}_q^n) \to \mathbb{Q}$ such that for all $V, W \in \mathcal{V}(\mathbb{F}_q^n)$:

(R1) $0 \leq \rho(V) \leq \dim(V)$.

(R2) if $V \subseteq W$, then $\rho(V) \leq \rho(W)$.

(R3) $\rho(V + W) + \rho(V \cap W) \leq \rho(V) + \rho(W)$.

Then $M = (\mathbb{F}_q^n, \rho)$ is a q-polymatroid and ρ is a rank function.

Remark

The rank function ρ of a q-polymatroid is the q-analogue of the rank function of a polymatroid. If ρ is integer valued M is a q-matroid.

q-Polymatroid of Rank Metric Codes

Notation: $\mathcal{C}(V, c) := \{M \in \mathcal{C} \,:\, \text{colsp}(M) \subseteq V\}$ where $V \subseteq \mathbb{F}_q^n$.

Theorem (Gorla, Jurrius, López, Ravagnani, 2019)

Let $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$ be a rank metric code. Let $\rho : \mathcal{V}(\mathbb{F}_q^n) \to \mathbb{Q}$ where for $V \subseteq \mathbb{F}_q^n$,

$$\rho(V) := \frac{\dim \mathcal{C} - \dim \mathcal{C}(V^\perp, c)}{m}.$$

Then $M_{\mathcal{C}} = (\mathbb{F}_q^n, \rho)$ is a q-polymatroid. We say $M_{\mathcal{C}}$ is the column q-polymatroid of $\mathcal{C}$.

Theorem (Gorla et al.)

If $\mathcal{C}_1$ and $\mathcal{C}_2 \subseteq \mathbb{F}_q^{n\times m}$, with $m > n$. are equivalent rank metric codes then $M_{\mathcal{C}_1}$ and $M_{\mathcal{C}_2}$ are equal up to an isomorphism of $\mathbb{F}_q^n$.

Example

Let $\mathcal{C} \subseteq \mathbb{F}_2^{3\times 4}$, where

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

Then $\rho : \mathcal{V}(\mathbb{F}_2^3) \to \mathbb{Q}$, where $\rho(V) = \frac{4-\dim \mathcal{C}(V^\perp, c)}{4}$.
For all $M \in \mathcal{C}$, $\mathrm{rk}(M) = \dim \mathrm{colsp}(M) = 3$.
Therefore if $\dim V^\perp \leq 2$ then $\dim \mathcal{C}(V^\perp, c) = 0$ and if $V^\perp = \mathbb{F}_2^3$ then $\dim \mathcal{C}(V^\perp, c) = 4$. Hence

$$\rho(V) = \min\{\dim(V), 1\}$$

$M_{\mathcal{C}}$ is called the uniform q-matroid of rank 1 over $\mathbb{F}_2^3$.

q-polymatroid of MRD codes

Theorem (Gorla et al.)

Let $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$, with rank distance d. $\mathcal{C}$ is an MRD code if and only if its associated column q-polymatroid $M_{\mathcal{C}} = (\mathbb{F}_q^n, \rho)$ is the uniform q-matroid of rank $n-d+1$ over $\mathbb{F}_q^n$, i.e. $\rho(V) = \min\{\dim V, n-d+1\}$ for all $V \subseteq \mathbb{F}_q^n$.

Questions

Question:

What can q-polymatroids tell us about rank metric codes?

Flats of q-polymatroids

Definition

Let $M = (\mathbb{F}_q^n, \rho)$ be a q-polymatroid, $F \subseteq \mathbb{F}_q^n$ is a flat of M if for all $x \notin F$,

$$\rho(F + \langle x \rangle) > \rho(F).$$

Denote by $\mathcal{F}(M)$ the collection of flats of M.

Remark

The flats of M form a lattice under inclusion, where $F_1 \wedge F_2 := F_1 \cap F_2$ and $F_1 \vee F_2 := \mathrm{cl}(F_1 + F_2)$.

Generalized weights from q-polymatroids

Recall that given a rank metric code $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$, the generalized weights are defined as:

$$d_r(\mathcal{C}) = \frac{1}{m}\min\{\dim A \,|\, A \in \mathcal{A}_q(n,m), \dim \mathcal{C} \cap A \geq r\}.$$

Theorem (Gluesing-Luerssen, J.)

Let $\mathcal{C} \subseteq \mathbb{F}_q^{n\times m}$, with $m > n$, be a rank metric code, $M_{\mathcal{C}}$ be its associated q-polymatroid and $\mathcal{F}(M)$ its collection of flats. The r-th generalized weight of $\mathcal{C}$ is given by

$$d_r(\mathcal{C}) = n - \max\{\dim(F) \,|\, F \in \mathcal{F}(M)\,,\, \rho(\mathbb{F}_q^n) - \rho(F) \geq r/m\}.$$

Example

Let $\mathcal{C} \subseteq \mathbb{F}_q^{n \times m}$, with $m > n$, be an MRD code and $M_{\mathcal{C}}$ be its associated column q-polymatroid. Then $M_{\mathcal{C}} = (\mathbb{F}_q^n, \rho)$ where for all $V \subseteq \mathbb{F}_q^n$,

$$\rho(V) = \min\{\dim V, n - d + 1\}$$

The flats of $M_{\mathcal{C}}$:

$$\mathcal{F}(M_{\mathcal{C}}) = \{F \subseteq \mathbb{F}_q^n \,:\, \dim(F) < n - d + 1\} \cup \mathbb{F}_q^n$$

Then from the flat theorem we get

$$d_r(\mathcal{C}) = d + \left\lfloor \frac{r}{m} \right\rfloor$$

Further Comments/Questions

- The rank weight enumerator of $\mathcal{C}$ can also be determined from the q-polymatroid (Shiromoto / Byrne et al.) .
- The notion of deletion/contraction of a q-polymatroid is equivalent to the notion of puncturing/shortening of a code.
- What other rank metric code invariants can be determined from the associated q-polymatroid?

References


E. Gorla , R. Jurrius, H. López, A. Ravagnani
Rank-metric codes and q-polymatroids.
Journal of Algebraic Combinatorics, pages 1-19, 2019


A. Ravagnani.
Generalized weights: an anticode approach.
CoRR, abs/1410.7207, 2014.


H. Gluesing-Luerssen, B. Jany.
q-Polymatroids and their relation to rank-metric codes.
arXiv:2104.06570v1 , 2021


E. Byrne, M. Ceria, S. Ionica, R. Jurrius
Weighted Subspace Designs from q-Polymatroids.
arXiv:2104.12463v1, 2021


K. Shiromoto
Matroids and Codes with the Rank Metric
Des. Codes Cryptogr., 87:1765-1776, 2019