Generalized rank weights and Betti numbers

Rakhi Pratihar

INRIA Saclay

Based on joint work with Trygve Johnsen and Hugues Verdure (UiT, Norway)

JOURNÉES C2 2023

October, Najac

Overview

Linear Codes: A Quick Review

Let q be a prime power and $\mathbb{F}_q$ be the finite field with q elements.

- An $[n, k]_q$ q-ary linear code $\mathcal{C}$ of length n and dimension k is a k-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$.

Linear Codes: A Quick Review

Let q be a prime power and $\mathbb{F}_q$ be the finite field with q elements.

- An $[n,k]_q$ q-ary linear code $\mathcal{C}$ of length n and dimension k is a k-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$.
- The Hamming support and the Hamming weight of a codeword $\mathbf{c} = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$ is:

$$\mathrm{Supp}(\mathbf{c}) = \{\mathrm{i} \colon \mathrm{c_i} \neq 0\} \text{ and } \mathrm{wt_H}(\mathbf{c}) = |\mathrm{Supp}(\mathbf{c})|.$$

Linear Codes: A Quick Review

Let q be a prime power and $\mathbb{F}_q$ be the finite field with q elements.

- An $[n,k]_q$ q-ary linear code $\mathcal{C}$ of length n and dimension k is a k-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$.
- The Hamming support and the Hamming weight of a codeword $\mathbf{c} = (c_1, \ldots, c_n) \in \mathbb{F}_q^n$ is:
$$\mathrm{Supp}(\mathbf{c}) = \{\mathrm{i} \colon \mathrm{c_i} \neq 0\} \text{ and } \mathrm{wt_H}(\mathbf{c}) = |\mathrm{Supp}(\mathbf{c})|.$$
- The support and support weight of a subcode $\mathcal{D}$ of $\mathcal{C}$ is
$$\mathrm{Supp}(\mathcal{D}) = \{\mathrm{i} \colon \exists \mathrm{d} = (\mathrm{d_1}, \ldots, \mathrm{d_n}) \in \mathcal{D},\ \mathrm{d_i} \neq 0\},\ \mathrm{wt}(\mathcal{D}) = |\mathrm{Supp}(\mathcal{D})|.$$

Linear Codes: A Quick Review

Let q be a prime power and $\mathbb{F}_q$ be the finite field with q elements.

- An $[n, k]_q$ q-ary linear code $\mathcal{C}$ of length n and dimension k is a k-dimensional $\mathbb{F}_q$-subspace of $\mathbb{F}_q^n$.
- The Hamming support and the Hamming weight of a codeword $\mathbf{c} = (c_1, \dots, c_n) \in \mathbb{F}_q^n$ is:
$$\mathrm{Supp}(\mathbf{c}) = \{\mathrm{i} \colon \mathrm{c_i} \neq 0\} \text{ and } \mathrm{wt_H}(\mathbf{c}) = |\mathrm{Supp}(\mathbf{c})|.$$
- The support and support weight of a subcode $\mathcal{D}$ of $\mathcal{C}$ is
$$\mathrm{Supp}(\mathcal{D}) = \{\mathrm{i} \colon \exists \mathrm{d} = (\mathrm{d_1}, \dots, \mathrm{d_n}) \in \mathcal{D},\ \mathrm{d_i} \neq 0\},\ \mathrm{wt}(\mathcal{D}) = |\mathrm{Supp}(\mathcal{D})|.$$
- The r^{th} generalized Hamming weight of $\mathcal{C}$ is
$$d_r(\mathcal{C}) := \min\{\mathrm{wt}(\mathcal{D}) \colon \mathcal{D} \text{ subcode of } \mathcal{C} \text{ with } \dim(\mathcal{D}) = \mathrm{r}\}.$$

Linear Codes: Basic Notions

For an $[n, k, d]_q$-linear code $\mathcal{C}$,

- $G \in M_{k\times n}(\mathbb{F}_q)$ is a generator matrix of $\mathcal{C}$ if $\mathcal{C} = \{\mathbf{x}G : \mathbf{x} \in \mathbb{F}_q^k\}$. Thus $\mathrm{rank(G) = k}$ and $\mathcal{C} = \mathrm{rowsp_{\mathbb{F}_q}(G)}$.
- $H \in M_{n-k\times n}(\mathbb{F}_q)$ is a parity check matrix of $\mathcal{C}$ if $H\mathbf{c}^T = 0 \,\forall\, \mathbf{c} \in G$. Thus $\mathrm{rank(H) = n - k}$ and $\mathcal{C}$ is the null space of H.

Linear Codes: Basic Notions

For an $[n, k, d]_q$-linear code $\mathcal{C}$,

- $G \in M_{k\times n}(\mathbb{F}_q)$ is a generator matrix of $\mathcal{C}$ if $\mathcal{C} = \{\mathbf{x}G : \mathbf{x} \in \mathbb{F}_q^k\}$. Thus $\mathrm{rank(G) = k}$ and $\mathcal{C} = \mathrm{rowsp_{\mathbb{F}_q}(G)}$.
- $H \in M_{n-k\times n}(\mathbb{F}_q)$ is a parity check matrix of $\mathcal{C}$ if $H\mathbf{c}^T = 0 \,\forall\, \mathbf{c} \in G$. Thus $\mathrm{rank(H) = n - k}$ and $\mathcal{C}$ is the null space of H.
- its weight enumerator polynomial is $W_{\mathcal{C}}(X, Y) = \sum_{i=0}^{n} A_i(\mathcal{C})X^{n-i}Y^i$ where $A_i(\mathcal{C}) := |\{\mathbf{c} \in \mathcal{C} : \mathrm{wt_H}(\mathbf{c}) = \mathrm{i}|$.

Linear Codes: Basic Notions

For an $[n, k, d]_q$-linear code $\mathcal{C}$,

- $G \in M_{k\times n}(\mathbb{F}_q)$ is a generator matrix of $\mathcal{C}$ if $\mathcal{C} = \{\mathbf{x}G : \mathbf{x} \in \mathbb{F}_q^k\}$. Thus $\mathrm{rank(G) = k}$ and $\mathcal{C} = \mathrm{rowsp_{\mathbb{F}_q}(G)}$.
- $H \in M_{n-k\times n}(\mathbb{F}_q)$ is a parity check matrix of $\mathcal{C}$ if $H\mathbf{c}^T = 0 \,\forall\, \mathbf{c} \in G$. Thus $\mathrm{rank(H) = n - k}$ and $\mathcal{C}$ is the null space of H.

- its weight enumerator polynomial is $W_{\mathcal{C}}(X, Y) = \sum_{i=0}^{n} A_i(\mathcal{C})X^{n-i}Y^i$ where $A_i(\mathcal{C}) := |\{\mathbf{c} \in \mathcal{C} : \mathrm{wt_H}(\mathbf{c}) = \mathrm{i}|$.

- the generalized weight enumerator polynomial is
$$W_{\mathcal{C}}^{(r)}(X, Y) = \sum_{i=0}^{n} A_i^{(r)}(\mathcal{C})X^{n-i}Y^i$$
where $A_i^{(r)}(\mathcal{C}) := |\{\mathcal{D}$ subcode of $\mathcal{C} : \mathrm{wt}(\mathcal{D}) = \mathrm{i}, \dim(\mathcal{D}) = \mathrm{r}\}|$.

Matroids Associated to Linear Codes

A matroid (via independent sets) is an ordered pair $(E, \mathcal{I})$ consisting of $E = [n] := \{1, \ldots, n\}$ and a collection $\mathcal{I}$ of subsets of E satisfying:

(I1) $\emptyset \in \mathcal{I}$.

(I2) If $I \in \mathcal{I}$ and $I' \subseteq I$, then $I' \in \mathcal{I}$.

(I3) If $I_1, I_2 \in \mathcal{I}$ with $|I_1| < |I_2|$, then there is an element $x \in I_2 \backslash I_1$, such that $I_1 \cup x \in \mathcal{I}$.

Matroids Associated to Linear Codes

A matroid (via independent sets) is an ordered pair $(E, \mathcal{I})$ consisting of $E = [n] := \{1, \ldots, n\}$ and a collection $\mathcal{I}$ of subsets of E satisfying:

(I1) $\emptyset \in \mathcal{I}$.

(I2) If $I \in \mathcal{I}$ and $I' \subseteq I$, then $I' \in \mathcal{I}$.

(I3) If $I_1, I_2 \in \mathcal{I}$ with $|I_1| < |I_2|$, then there is an element $x \in I_2 \backslash I_1$, such that $I_1 \cup x \in \mathcal{I}$.

Let $\mathcal{C}$ be an $[n, k]_q$-linear code with a parity check matrix $H = [H_1, \cdots, H_n]$, H_i's are the columns of H.

- The matroid associated to $\mathcal{C}$ is $M_{\mathcal{C}} = ([n], \mathcal{I})$ where

$$\mathcal{I} = \{\sigma \subseteq [n] \colon \{H_i \colon i \in \sigma\} \text{ are } \mathbb{F}_q\text{-linearly independent}\}.$$

Basic Properties of the Associated Matroid

- For any $\sigma \subseteq [n]$, its rank and nullity is defined as

$$\mathtt{r}(\sigma) = \max\{|\tau| : \tau \in \mathcal{I} \text{ and } \tau \subseteq \sigma\} \text{ and } \mathtt{n}(\sigma) = n - \mathtt{r}(\sigma).$$

- Thus $\mathtt{r}(M_{\mathcal{C}}) = n - k$ and $\mathtt{n}(M_{\mathcal{C}}) = k$.

Basic Properties of the Associated Matroid

- For any $\sigma \subseteq [n]$, its rank and nullity is defined as

$$\mathrm{r}(\sigma) = \max\{|\tau| : \tau \in \mathcal{I} \text{ and } \tau \subseteq \sigma\} \text{ and } \mathrm{n}(\sigma) = n - \mathrm{r}(\sigma).$$

- Thus $\mathrm{r}(M_{\mathcal{C}}) = n - k$ and $\mathrm{n}(M_{\mathcal{C}}) = k$.
- The dual matroid is the matroid $M^* = (E = [n], \mathrm{r}^*)$, where

$$\mathrm{r}^*(\sigma) = |\sigma| + \mathrm{r}(E \setminus \sigma) - \mathrm{r}(E).$$

Basic Properties of the Associated Matroid

- For any $\sigma \subseteq [n]$, its rank and nullity is defined as

$$\mathrm{r}(\sigma) = \max\{|\tau| : \tau \in \mathcal{I} \text{ and } \tau \subseteq \sigma\} \text{ and } \mathrm{n}(\sigma) = n - \mathrm{r}(\sigma).$$

- Thus $\mathrm{r}(M_{\mathcal{C}}) = n - k$ and $\mathrm{n}(M_{\mathcal{C}}) = k$.
- The dual matroid is the matroid $M^* = (E = [n], \mathrm{r}^*)$, where

$$\mathrm{r}^*(\sigma) = |\sigma| + \mathrm{r}(E \setminus \sigma) - \mathrm{r}(E).$$

- The matroid complex Δ_M is the simplicial complex on the vertex set $[n]$ whose faces are the independent sets of $M_{\mathcal{C}}$.

Lattices of Flats and Cycles of a Matroid

- Flats are subsets $\sigma \subseteq E$ such that $\mathrm{r}(\sigma \cup \{x\}) = \mathrm{r}(\sigma) + 1$ for all $x \in E \backslash \sigma$.
- Cycles of nullity i are the minimal (w.r.t. inclusion) elements of N_i, where

$$N_i = \{\sigma \subseteq [n] \colon \mathrm{n}(\sigma) = i\}.$$

Lemma

- *The cycles (resp. flats) of a matroid M form a lattice. We denote these lattices by $L_C(M)$ and $L_F(M)$, respectively.*

Lattices of Flats and Cycles of a Matroid

- Flats are subsets $\sigma \subseteq E$ such that $\mathrm{r}(\sigma \cup \{x\}) = \mathrm{r}(\sigma) + 1$ for all $x \in E \backslash \sigma$.
- Cycles of nullity i are the minimal (w.r.t. inclusion) elements of N_i, where

$$N_i = \{\sigma \subseteq [n] \colon \mathrm{n}(\sigma) = i\}.$$

Lemma

- *The cycles (resp. flats) of a matroid M form a lattice. We denote these lattices by $L_C(M)$ and $L_F(M)$, respectively.*
- *(Duality) σ is a flat of M of rank r if and only if $E \setminus \sigma$ is of a cycle of the dual matroid M^* of nullity $n - r$.*

J. Oxley, Matroid Theory, 2014.

Stanley-Reisner Ring Associated to a Matroid

To the matroid complex $\Delta_M = ([n], \mathcal{I})$ corresponding to $M_{\mathcal{C}}$, one can associate the Stanley-Reisner ideal

$$I_\Delta := \text{ the ideal of } R := \mathbb{F}_q[X_1, \ldots, X_n] \text{ generated by } \{\prod_{i \in \tau} X_i : \tau \notin \mathcal{I}\},$$

Stanley-Reisner Ring Associated to a Matroid

To the matroid complex $\Delta_M = ([n], \mathcal{I})$ corresponding to $M_{\mathcal{C}}$, one can associate the Stanley-Reisner ideal

$$I_\Delta := \text{ the ideal of } R := \mathbb{F}_q[X_1, \ldots, X_n] \text{ generated by } \{\prod_{i \in \tau} X_i \colon \tau \notin \mathcal{I}\},$$

and $R_\Delta := R/I_\Delta$ is the Stanley-Reisner ring of Δ or more generally, of $M_{\mathcal{C}}$.

Stanley-Reisner Ring Associated to a Matroid

To the matroid complex $\Delta_M = ([n], \mathcal{I})$ corresponding to $M_{\mathcal{C}}$, one can associate the Stanley-Reisner ideal

$$I_\Delta := \text{ the ideal of } R := \mathbb{F}_q[X_1, \ldots, X_n] \text{ generated by } \{\prod_{i \in \tau} X_i : \tau \notin \mathcal{I}\},$$

and $R_\Delta := R/I_\Delta$ is the Stanley-Reisner ring of Δ or more generally, of $M_{\mathcal{C}}$.

R_Δ is a finitely generated $\mathbb{F}_q$-algebra of dimension $n-k$. Since matroid complexes are shellable, R_Δ is Cohen-Macaulay.

Stanley-Reisner Ring Associated to a Matroid

To the matroid complex $\Delta_M = ([n], \mathcal{I})$ corresponding to $M_{\mathcal{C}}$, one can associate the Stanley-Reisner ideal

$$I_\Delta := \text{ the ideal of } R := \mathbb{F}_q[X_1, \ldots, X_n] \text{ generated by } \{\prod_{i \in \tau} X_i \colon \tau \notin \mathcal{I}\},$$

and $R_\Delta := R/I_\Delta$ is the Stanley-Reisner ring of Δ or more generally, of $M_{\mathcal{C}}$.

R_Δ is a finitely generated $\mathbb{F}_q$-algebra of dimension $n-k$. Since matroid complexes are shellable, R_Δ is Cohen-Macaulay. Thus R_Δ has a minimal free resolution

$$F_k \to \cdots \to F_i \to F_0 \to R_\Delta \to 0, \text{ where}$$

$$F_0 = R = \mathbb{F}_q[X_1, \ldots, X_n] \text{ and } F_i = \bigoplus_{j \in \mathbb{Z}} R(-j)^{\beta_{i,j}} \text{ for } i = 0, 1, \ldots, k.$$

Generalized Hamming Weights and Betti numbers

Let $\beta_{i,j}$'s are $\mathbb{N}$-graded Betti numbers of the Stanley-Reisner ring of $M_{\mathcal{C}}$.

Generalized Hamming Weights and Betti numbers

Let $\beta_{i,j}$'s are $\mathbb{N}$-graded Betti numbers of the Stanley-Reisner ring of $M_{\mathcal{C}}$.

Lemma (Johnsen - Verdure, 2013)

$\beta_{i,j} \neq 0$ if and only if $\exists$ a cycle σ of $M_{\mathcal{C}}$ of nullity i and $|\sigma| = j$.

Generalized Hamming Weights and Betti numbers

Let $\beta_{i,j}$'s are $\mathbb{N}$-graded Betti numbers of the Stanley-Reisner ring of $M_{\mathcal{C}}$.

Lemma (Johnsen - Verdure, 2013)

$\beta_{i,j} \neq 0$ *if and only if* $\exists$ *a cycle* σ *of* $M_{\mathcal{C}}$ *of nullity* i *and* $|\sigma| = j$.

Theorem (Johnsen - Verdure, 2013)

The generalized weights of $\mathcal{C}$ *are given by*

$$d_i = \min\{j : \beta_{i,j} \neq 0\}, \quad 0 \leq i \leq n - r(M_{\mathcal{C}}).$$

T. Johnsen, H. Verdure, Hamming weights and Betti numbers of Stanley–Reisner rings associated to matroids, Appl. Algebra Engg. Commun. Comput., 2013.

Concluding the case of Hamming metric codes

The Möbius function of a finite poset (partially ordered set) $(P, \preceq)$ is

$$\mu(x, x) = 1 \text{ for all } x \in P, \text{ and } \mu(x, z) = -\sum_{x \preceq y \prec z} \mu(x, y) \forall\, x \prec z \text{ in } P.$$

Concluding the case of Hamming metric codes

The Möbius function of a finite poset (partially ordered set) $(P, \preceq)$ is

$$\mu(x,x) = 1 \text{ for all } x \in P, \text{ and } \mu(x,z) = -\sum_{x \preceq y \prec z} \mu(x,y) \forall\, x \prec z \text{ in } P.$$

Theorem (Stanley, 1977)

For a matroid $M = (E, r)$ and a subset $X \subseteq E$,

$$\beta_{n(X),X} = (-1)^{n(X)} \mu_{L_F(M^*)}(E \backslash X, E) = (-1)^{n(X)} \mu_{L_C(M)}(\emptyset, X),$$

$L_F(M^*)$ and $L_C(M)$ are the lattices of flats of M^* and cycles of M, resp.

Concluding the case of Hamming metric codes

The Möbius function of a finite poset (partially ordered set) $(P, \preceq)$ is

$$\mu(x,x) = 1 \text{ for all } x \in P, \text{ and } \mu(x,z) = -\sum_{x \preceq y \prec z} \mu(x,y) \forall\, x \prec z \text{ in } P.$$

Theorem (Stanley, 1977)

For a matroid $M = (E, r)$ and a subset $X \subseteq E$,

$$\beta_{n(X),X} = (-1)^{n(X)} \mu_{L_F(M^*)}(E \backslash X, E) = (-1)^{n(X)} \mu_{L_C(M)}(\emptyset, X),$$

$L_F(M^*)$ and $L_C(M)$ are the lattices of flats of M^* and cycles of M, resp.

$$\left\{ \begin{array}{c} \text{Cycles of the associated} \\ \text{parity-check matroid } M_{\mathcal{C}} \end{array} \right\} \Rightarrow \left\{ \begin{array}{c} \text{Generalized Hamming} \\ \text{weights, higher weight} \\ \text{spectra of } \mathcal{C} \end{array} \right\}$$

Vector rank metric codes

- An $[n, k]$ vector rank metric code $\mathcal{C}$ over $\mathbb{F}_{q^m}/\mathbb{F}_q$ of length n and dimension k is a k-dimensional $\mathbb{F}_{q^m}$-subspace of $\mathbb{F}_{q^m}^n$.
- The rank distance between two codewords $f, g \in \mathcal{C}$

$$rank(f, g) = \dim_{\mathbb{F}_q} \langle f_i - g_i : i \in [n] \rangle_{\mathbb{F}_q},.$$

Vector rank metric codes

- An $[n, k]$ vector rank metric code $\mathcal{C}$ over $\mathbb{F}_{q^m}/\mathbb{F}_q$ of length n and dimension k is a k-dimensional $\mathbb{F}_{q^m}$-subspace of $\mathbb{F}_{q^m}^n$.
- The rank distance between two codewords $f, g \in \mathcal{C}$

$$rank(f, g) = \dim_{\mathbb{F}_q} \langle f_i - g_i : i \in [n] \rangle_{\mathbb{F}_q},.$$

- Let $M_B(c)$ be the coordinate matrix of a codeword $c \in \mathcal{C}$ w.r.t. a fixed $\mathbb{F}_q$-basis B of $\mathbb{F}_{q^m}$.
- $\mathrm{Rsupp(c)}$:=$\mathbb{F}_q$-row space of $M_B(c)$, $wt_R(c) := \dim_{\mathbb{F}_q} \mathrm{Rsupp(c)}$.
- For $\mathcal{D} \subseteq \mathcal{C}$, $\mathrm{Rsupp}(\mathcal{D})$:= F_q-linear span of $\{\mathrm{Rsupp(d)} : \mathrm{d} \in \mathcal{D}\}$.

Vector rank metric codes

- An $[n, k]$ vector rank metric code $\mathcal{C}$ over $\mathbb{F}_{q^m}/\mathbb{F}_q$ of length n and dimension k is a k-dimensional $\mathbb{F}_{q^m}$-subspace of $\mathbb{F}_{q^m}^n$.
- The rank distance between two codewords $f, g \in \mathcal{C}$

$$rank(f, g) = \dim_{\mathbb{F}_q} \langle f_i - g_i : i \in [n] \rangle_{\mathbb{F}_q},.$$

- Let $M_B(c)$ be the coordinate matrix of a codeword $c \in \mathcal{C}$ w.r.t. a fixed $\mathbb{F}_q$-basis B of $\mathbb{F}_{q^m}$.
- $\mathrm{Rsupp(c)}$:=$\mathbb{F}_q$-row space of $M_B(c)$, $wt_R(c) := \dim_{\mathbb{F}_q} \mathrm{Rsupp(c)}$.
- For $\mathcal{D} \subseteq \mathcal{C}$, $\mathrm{Rsupp}(\mathcal{D})$:= F_q-linear span of $\{\mathrm{Rsupp(d) : d} \in \mathcal{D}\}$.
- The r^{th} generalized rank weight of $\mathcal{C}$

$$d_r = \min\{\dim_{\mathbb{F}_q} \mathrm{Rsupp}(\mathcal{D}), \mathcal{D} \subseteq \mathcal{C} \text{ with } \dim_{\mathbb{F}_{q^m}}(\mathcal{D}) = \mathrm{r}\}.$$

q-Matroids via Rank Functions

$\mathcal{E} = \mathbb{F}_q^n, \quad \mathcal{L}(\mathcal{E}) = \{\mathbb{F}_q\text{- linear subspaces of } \mathcal{E}\}$

A q-matroid $\mathcal{M}$ is a pair $(\mathcal{E}, \rho)$ consisting of $\mathcal{E} = \mathbb{F}_q^n$ and $\rho : \mathcal{L}(\mathcal{E}) \to \mathbb{Z}$ satisfying the following axioms: for any $U, V \in \mathcal{L}(\mathcal{E})$

(R1) (Boundedness) $0 \leq \rho(U) \leq \dim U$.

(R2) (Monotonicity) If $U \subseteq V$, then $\rho(U) \leq \rho(V)$.

(R3) (Submodularity) $\rho(U+V) + \rho(U \cap V) \leq \rho(U) + \rho(V)$.

q-Matroids via Rank Functions

$\mathcal{E} = \mathbb{F}_q^n$, $\quad \mathcal{L}(\mathcal{E}) = \{\mathbb{F}_q$- linear subspaces of $\mathcal{E}\}$

A q-matroid $\mathcal{M}$ is a pair $(\mathcal{E}, \rho)$ consisting of $\mathcal{E} = \mathbb{F}_q^n$ and $\rho : \mathcal{L}(\mathcal{E}) \to \mathbb{Z}$ satisfying the following axioms: for any $U, V \in \mathcal{L}(\mathcal{E})$

(R1) (Boundedness) $0 \leq \rho(U) \leq \dim U$.

(R2) (Monotonicity) If $U \subseteq V$, then $\rho(U) \leq \rho(V)$.

(R3) (Submodularity) $\rho(U+V) + \rho(U \cap V) \leq \rho(U) + \rho(V)$.

For a q-matroid $\mathcal{M} = (\mathcal{E}, \rho)$,

- independent spaces : $\mathcal{I}_\rho := \{U \in \mathcal{L}(\mathcal{E}) \colon \rho(U) = \dim U\}$.

q-Matroids via Rank Functions

$\mathcal{E} = \mathbb{F}_q^n, \quad \mathcal{L}(\mathcal{E}) = \{\mathbb{F}_q$- linear subspaces of $\mathcal{E}\}$

A q-matroid $\mathcal{M}$ is a pair $(\mathcal{E}, \rho)$ consisting of $\mathcal{E} = \mathbb{F}_q^n$ and $\rho : \mathcal{L}(\mathcal{E}) \to \mathbb{Z}$ satisfying the following axioms: for any $U, V \in \mathcal{L}(\mathcal{E})$

(R1) (Boundedness) $0 \leq \rho(U) \leq \dim U$.

(R2) (Monotonicity) If $U \subseteq V$, then $\rho(U) \leq \rho(V)$.

(R3) (Submodularity) $\rho(U+V) + \rho(U \cap V) \leq \rho(U) + \rho(V)$.

For a q-matroid $\mathcal{M} = (\mathcal{E}, \rho)$,

- independent spaces : $\mathcal{I}_\rho := \{U \in \mathcal{L}(\mathcal{E}) \colon \rho(U) = \dim U\}$.
- dual q-matroid : $\mathcal{M}^* = (\mathcal{E}, \rho^*)$, $\rho^*(U) = \dim U + \rho(U^\perp) - \rho(\mathcal{E})$.

q-Matroids via Rank Functions

$\mathcal{E} = \mathbb{F}_q^n$, $\quad \mathcal{L}(\mathcal{E}) = \{\mathbb{F}_q$- linear subspaces of $\mathcal{E}\}$

A q-matroid $\mathcal{M}$ is a pair $(\mathcal{E}, \rho)$ consisting of $\mathcal{E} = \mathbb{F}_q^n$ and $\rho : \mathcal{L}(\mathcal{E}) \to \mathbb{Z}$ satisfying the following axioms: for any $U, V \in \mathcal{L}(\mathcal{E})$

(R1) (Boundedness) $0 \leq \rho(U) \leq \dim U$.

(R2) (Monotonicity) If $U \subseteq V$, then $\rho(U) \leq \rho(V)$.

(R3) (Submodularity) $\rho(U+V) + \rho(U \cap V) \leq \rho(U) + \rho(V)$.

For a q-matroid $\mathcal{M} = (\mathcal{E}, \rho)$,

- independent spaces : $\mathcal{I}_\rho := \{U \in \mathcal{L}(\mathcal{E})\colon \rho(U) = \dim U\}$.
- dual q-matroid : $\mathcal{M}^* = (\mathcal{E}, \rho^*)$, $\rho^*(U) = \dim U + \rho(U^\perp) - \rho(\mathcal{E})$.
- nullity function: $\eta : \mathcal{L}(\mathcal{E}) \to \mathbb{Z}$ given by $\eta(U) = \dim_{\mathbb{F}_q} U - \rho(U)$.

R. Jurrius and R. Pellikaan, Defining the q-analogue of a matroid, Electron. J. Combin., 2018.

q-Matroids Associated to Rank Metric Codes

Definition (Jurrius - Pellikaan, 2018)

Let $\mathcal{C} \leq \mathbb{F}_{q^m}^n$ be a vector rank metric code over $\mathbb{F}_{q^m}/\mathbb{F}_q$ with a generator matrix $G \in \mathbb{F}_{q^m}^{k \times n}$. The q-matroid associated to $\mathcal{C}$ is $\mathcal{M}_{\mathcal{C}} = (\mathcal{E} = \mathbb{F}_q^n, \rho_{\mathcal{C}})$,

$$\rho_{\mathcal{C}}(J) := rank(GY^T) \text{ for } J \leq \mathbb{F}_q^n,$$

where Y is a generator matrix of J.

q-Matroids Associated to Rank Metric Codes

Definition (Jurrius - Pellikaan, 2018)

Let $\mathcal{C} \leq \mathbb{F}_{q^m}^n$ be a vector rank metric code over $\mathbb{F}_{q^m}/\mathbb{F}_q$ with a generator matrix $G \in \mathbb{F}_{q^m}^{k\times n}$. The q-matroid associated to $\mathcal{C}$ is $\mathcal{M}_\mathcal{C} = (\mathcal{E} = \mathbb{F}_q^n, \rho_\mathcal{C})$,

$$\rho_\mathcal{C}(J) := rank(GY^T) \text{ for } J \leq \mathbb{F}_q^n,$$

where Y is a generator matrix of J.

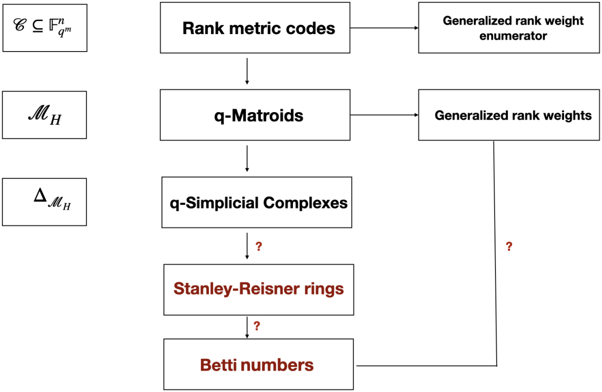
Lemma

Let $\mathcal{C}$ be a Gabidulin rank metric code. For any $X \leq \mathcal{E}$, define

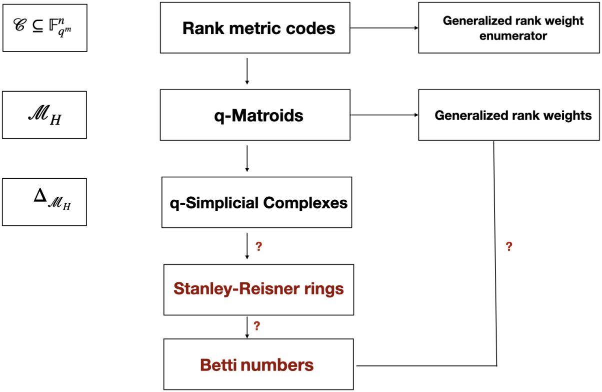
$$\rho_\mathcal{C}(X) := \dim_{\mathbb{F}_{q^m}}(\mathcal{C}) - \dim_{\mathbb{F}_{q^m}}(\mathcal{C}(X^\perp)),$$

where $\mathcal{C}(X^\perp) = \{c \in \mathcal{C} : \mathrm{Rsupp(c)} \leq \mathrm{X}^\perp\}$. Then $(\mathcal{E}, \rho_\mathcal{C})$ is a q-matroid.

Question


$\mathscr{C} \subseteq \mathbb{F}_{q^m}^n$
Rank metric codes
Generalized rank weight enumerator
$\mathscr{M}_H$
q-Matroids
Generalized rank weights
$\Delta_{\mathscr{M}_H}$
q-Simplicial Complexes
?
Stanley-Reisner rings
?
Betti numbers
?

Question



Can something like Betti numbers be defined in the context of rank metric codes, or more generally, for q-matroids that can be related to the generalized rank weights?

Classical Matroid associated to a q-Matroid

Definition

To a q-matroid $\mathcal{M} = (\mathcal{E}, \rho)$, we associate a pair $Cl(\mathcal{M}) := (P(\mathcal{E}), r_\rho)$,

- $P(\mathcal{E})$ is the set of all 1-dimensional subspaces of $\mathcal{E}$,
- $r_\rho(S) := \rho(\langle S \rangle)$, for $S \subseteq P(\mathcal{E})$, where $\langle S \rangle \subseteq \mathcal{E}$ is the linear $\mathbb{F}_q$-space spanned by elements in S.

Classical Matroid associated to a q-Matroid

Definition

To a q-matroid $\mathcal{M} = (\mathcal{E}, \rho)$, we associate a pair $Cl(\mathcal{M}) := (P(\mathcal{E}), r_\rho)$,

- $P(\mathcal{E})$ is the set of all 1-dimensional subspaces of $\mathcal{E}$,
- $r_\rho(S) := \rho(\langle S \rangle)$, for $S \subseteq P(\mathcal{E})$, where $\langle S \rangle \subseteq \mathcal{E}$ is the linear $\mathbb{F}_q$-space spanned by elements in S.

Lemma

$Cl(\mathcal{M}) = (P(\mathcal{E}), r_\rho)$ is a matroid.

$Cl(\mathcal{M})$ is called the classical matroid associated to $\mathcal{M}$ or projectivization matroid of the q-matroid $\mathcal{M}$.

T. Johnsen, R. Pratihar, and H. Verdure, Weight spectra of Gabidulin rank metric codes and Betti numbers, São Paulo J. Math. Sci., 2022.

Cycles of the associated classical matroid

- q-Cycles of $\mathcal{M}$ of nullity i: minimal elements (w.r.t. inclusion) of
$$N_i = \{U \subseteq \mathcal{E} : \eta(U) = i\} \quad \text{for } 0 \le i \le \eta(\mathcal{E}).$$
- q-flats: subspaces $U \subseteq \mathcal{E}$ such that $\rho(U \oplus \langle e \rangle) > \rho(U)\ \forall\ e \in \mathcal{E} \backslash U$.

Cycles of the associated classical matroid

- q-Cycles of $\mathcal{M}$ of nullity i: minimal elements (w.r.t. inclusion) of
$$N_i = \{U \subseteq \mathcal{E} : \eta(U) = i\} \quad \text{for } 0 \leq i \leq \eta(\mathcal{E}).$$
- q-flats: subspaces $U \subseteq \mathcal{E}$ such that $\rho(U \oplus \langle e \rangle) > \rho(U)\ \forall\ e \in \mathcal{E} \backslash U$.

Theorem (Johnsen, P., Verdure, 2022)

The lattice of q-flats of $\mathcal{M}$ is isomorphic to the lattice of flats of $Cl(\mathcal{M})$. Dually,

$$L_C(\mathcal{M}^*) \cong L_C(Cl(\mathcal{M})^*)$$
$$U \longmapsto R(U) = P(\mathcal{E}) \setminus P(U^\perp)$$

Cycles of the associated classical matroid

- *q*-Cycles of $\mathcal{M}$ of nullity i: minimal elements (w.r.t. inclusion) of
$$N_i = \{U \subseteq \mathcal{E} : \eta(U) = i\} \quad \text{for } 0 \leq i \leq \eta(\mathcal{E}).$$
- *q*-flats: subspaces $U \subseteq \mathcal{E}$ such that $\rho(U \oplus \langle e \rangle) > \rho(U)\ \forall\ e \in \mathcal{E} \setminus U$.

Theorem (Johnsen, P., Verdure, 2022)

The lattice of q-flats of $\mathcal{M}$ is isomorphic to the lattice of flats of $Cl(\mathcal{M})$. Dually,

$$L_C(\mathcal{M}^*) \cong L_C(Cl(\mathcal{M})^*)$$
$$U \longmapsto R(U) = P(\mathcal{E}) \setminus P(U^{\perp})$$

Generalized rank weights and Betti numbers

Lemma (Shiromoto, 2016, Johnsen - Ghorpade, 2020)

For a Gabidulin rank metric code $\mathcal{C}$ *over* $\mathbb{F}_{q^m}/\mathbb{F}_q$,

$$d_r(\mathcal{C}) = \min\{\dim_{\mathbb{F}_q} X : X \subseteq \mathbb{F}_q^n \text{ with } \eta^*_{\mathcal{C}}(X) = r\}.$$

where $\eta^*_{\mathcal{C}}$ *is the nullity function of the dual q-matroid* $\mathcal{M}_{\mathcal{C}}{}^*$.

Generalized rank weights and Betti numbers

Lemma (Shiromoto, 2016, Johnsen - Ghorpade, 2020)

For a Gabidulin rank metric code $\mathcal{C}$ over $\mathbb{F}_{q^m}/\mathbb{F}_q$,

$$d_r(\mathcal{C}) = \min\{\dim_{\mathbb{F}_q} X : X \subseteq \mathbb{F}_q^n \text{ with } \eta_{\mathcal{C}}^*(X) = r\}.$$

where $\eta_{\mathcal{C}}^*$ is the nullity function of the dual q-matroid $\mathcal{M}_{\mathcal{C}}{}^*$.

Theorem (Johnsen, P., Verdure, 2022)

The r^{th} generalized rank weight of a Gabidulin rank metric code is

$$d_r = \min\{j | \beta_{r,(j)_q} \neq 0\}, \text{ where } (j)_q = q^{n-1} + \ldots + q^{n-j}$$

and $\beta_{i,(j)_q}$'s are the $\mathbb{N}-$graded Betti numbers of the Stanley-Reisner ring associated to $Cl(\mathcal{M}_{\mathcal{C}})^*$.

Weight spectra in terms of Betti numbers

- Let $Q = q^m$, $\tilde{Q} = Q^r$ and $\tilde{\mathcal{C}} = \mathcal{C} \otimes_{\mathbb{F}_Q} \mathbb{F}_{\tilde{Q}}$.
- $A_{\mathcal{C},s}(\tilde{Q})$ - the number of codewords of rank weight s in $\tilde{\mathcal{C}}$.
- $A^{(i)}_{\mathcal{C},s}(\tilde{Q})$ - the number of subcodes $\mathcal{D} \subseteq \tilde{\mathcal{C}}$ of dimension i with rank support weight s.

Weight spectra in terms of Betti numbers

- Let $Q = q^m$, $\tilde{Q} = Q^r$ and $\tilde{\mathcal{C}} = \mathcal{C} \otimes_{\mathbb{F}_Q} \mathbb{F}_{\tilde{Q}}$.
- $A_{\mathcal{C},s}(\tilde{Q})$ - the number of codewords of rank weight s in $\tilde{\mathcal{C}}$.
- $A^{(i)}_{\mathcal{C},s}(\tilde{Q})$ - the number of subcodes $\mathcal{D} \subseteq \tilde{\mathcal{C}}$ of dimension i with rank support weight s.

Theorem (Johnsen, P., Verdure, 2022)

Let $N = Cl(\mathcal{M})^*$. *Then*

$$A_{\mathcal{C},s}(\tilde{Q}) = \sum_{l=0}^{k} \sum_{i=0}^{k} (-1)^i (\beta^{(l)}_{i,(s)_q}(N) - \beta^{(l-1)}_{i,(s)_q}(N)) \tilde{Q}^l.$$

Weight spectra in terms of Betti numbers

- Let $Q = q^m$, $\tilde{Q} = Q^r$ and $\tilde{\mathcal{C}} = \mathcal{C} \otimes_{\mathbb{F}_Q} \mathbb{F}_{\tilde{Q}}$.
- $A_{\mathcal{C},s}(\tilde{Q})$ - the number of codewords of rank weight s in $\tilde{\mathcal{C}}$.
- $A^{(i)}_{\mathcal{C},s}(\tilde{Q})$ - the number of subcodes $\mathcal{D} \subseteq \tilde{\mathcal{C}}$ of dimension i with rank support weight s.

Theorem (Johnsen, P., Verdure, 2022)

Let $N = Cl(\mathcal{M})^*$. Then

$$A_{\mathcal{C},s}(\tilde{Q}) = \sum_{l=0}^{k} \sum_{i=0}^{k} (-1)^i (\beta^{(l)}_{i,(s)_q}(N) - \beta^{(l-1)}_{i,(s)_q}(N)) \tilde{Q}^l.$$

The higher weight spectra can be determined from the following relation

$$A_{\mathcal{C},s}(\tilde{Q}) = \sum_{i=0}^{k} [r, i]_{q^m} A^{(i)}_{\mathcal{C},s}(Q),$$

where $[r, i]_{q^m}$ is the number of F_{q^m}-linear subspaces of dimension i contained in $F^r_{q^m}$.

Virtual Betti numbers of a q-matroid

Definition (Virtual Betti numbers)

- $V_{i,U}(\mathcal{M}^*) := \beta_{i,R(U)}(Cl(\mathcal{M})^*) = (-1)^{\eta^*(U)}\mu_{L_C(\mathcal{M}^*)}(0,U)$, where $\mu_{L_C(\mathcal{M}^*)}$ is the Möbius function on the lattice of q-cycles $L_C(\mathcal{M}^*)$.

Virtual Betti numbers of a q-matroid

Definition (Virtual Betti numbers)

- $V_{i,U}(\mathcal{M}^*) := \beta_{i,R(U)}(Cl(\mathcal{M})^*) = (-1)^{\eta^*(U)}\mu_{L_C(\mathcal{M}^*)}(0,U)$, where $\mu_{L_C(\mathcal{M}^*)}$ is the Möbius function on the lattice of q-cycles $L_C(\mathcal{M}^*)$.
- (l^{th} elongated virtual $\mathbb{N}$-graded Betti numbers)

$$V_{i,j}^{(l)}(\mathcal{M}^*) := \sum_{\substack{\eta^*(U)=l+i,\\ \dim U=j}} V_{i,U}^{(l)} \text{ and thus } \beta_{i,(j)_q}^{(l)}(Cl(\mathcal{M})^*) = V_{i,j}^{(l)}.$$

Virtual Betti numbers of a q-matroid

Definition (Virtual Betti numbers)

- $V_{i,U}(\mathcal{M}^*) := \beta_{i,R(U)}(Cl(\mathcal{M})^*) = (-1)^{\eta^*(U)}\mu_{L_C(\mathcal{M}^*)}(0,U)$, where $\mu_{L_C(\mathcal{M}^*)}$ is the Möbius function on the lattice of q-cycles $L_C(\mathcal{M}^*)$.
- (l^{th} elongated virtual $\mathbb{N}$-graded Betti numbers)

$$V_{i,j}^{(l)}(\mathcal{M}^*) := \sum_{\substack{\eta^*(U)=l+i,\\ \dim U=j}} V_{i,U}^{(l)} \text{ and thus } \beta_{i,(j)_q}^{(l)}(Cl(\mathcal{M})^*) = V_{i,j}^{(l)}.$$

$$\left\{ \begin{array}{c} q\text{-Cycles of the} \\ \text{dual } q\text{-matroid } \mathcal{M}_{\mathcal{C}}^* \end{array} \right\} \Rightarrow \left\{ \begin{array}{c} \text{Generalized rank weights,} \\ \text{higher weight spectra} \\ \text{of the rank metric code } \mathcal{C} \end{array} \right\}$$

Concluding Remarks

A topological approach to define Betti numbers for q-matroids ...

S. R. Ghorpade, R. Pratihar, and T. H. Randrianarisoa, Shellability and homology of q-complexes and q-matroids, J. Alg. Combin., 2022.

S. R. Ghorpade, R. Pratihar, T. H. Randrianarisoa, H. Verdure, G. Wilson, The homotopy and homology of q-matroid complexes, manuscript under preparation.

Concluding Remarks

A topological approach to define Betti numbers for q-matroids ...

- S. R. Ghorpade, R. Pratihar, and T. H. Randrianarisoa, Shellability and homology of q-complexes and q-matroids, J. Alg. Combin., 2022.
- S. R. Ghorpade, R. Pratihar, T. H. Randrianarisoa, H. Verdure, G. Wilson, The homotopy and homology of q-matroid complexes, manuscript under preparation.

Is there any relation between singular homology of a q-matroid equipped with the order topology and the virtual Betti numbers or the Möbius numbers?

Concluding Remarks

A topological approach to define Betti numbers for q-matroids ...

S. R. Ghorpade, R. Pratihar, and T. H. Randrianarisoa, Shellability and homology of q-complexes and q-matroids, J. Alg. Combin., 2022.

S. R. Ghorpade, R. Pratihar, T. H. Randrianarisoa, H. Verdure, G. Wilson, The homotopy and homology of q-matroid complexes, manuscript under preparation.

Is there any relation between singular homology of a q-matroid equipped with the order topology and the virtual Betti numbers or the Möbius numbers?

T. Johnsen, R. Pratihar, and T. H. Randrianarisoa, The Euler characteristic, q-matroids, and a Möbius function, arXiv preprint, 2023.

Open Questions

- Stanley-Reisner like ring associated to a q-matroid complex in a way that it reveals the some structural properties of a vector (Gabidulin) rank metric code.
- In connection with matrix rank metric codes, the study of q-polymatroids are of current interest. Can Betti numbers can be defined for q-polymatroids?
- Generalizing the notion of higher weight spectra of a linear code to matroids.

Thank you!