# The Characteristic polynomial of $q$-matroids

## Coding Theory and Cryptography
## A Conference in Honor of Joachim Rosenthal's 60th Birthday

Benjamin Jany

University of Kentucky

July 12, 2022

# Introduction

- Matroid theory has been intensively studied over the past 50 years because of its application to different areas of Mathematics, including the study of linear block codes.
- In recent years, its q-analogue, the q-matroid was reintroduced by Jurrius and Pellikaan [1] and has been found useful in studying rank metric codes.
- The Characteristic polynomial of a matroid induced by a block code captures important information of the latter object? Does the characteristic polynomial of $q$-matroid induced by a rank metric captures similar information?

# Outline

# The Hamming and rank metric

Let $\Gamma = \{\gamma_1, \ldots, \gamma_m\}$ be a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$.

Let $\Gamma(v) \in \mathbb{F}_q^{n \times m}$ such that its $i^{\text{th}}$ row is the coordinate vector of $v_i$ w.r.t $\Gamma$.

## Definition

Let $v \in \mathbb{F}_{q^m}^n$:

- Hamming weight: $w_H(v) := |\{i : v_i \neq 0\}|$.
- Rank weight: $w_R(v) := \text{rk}_{\mathbb{F}_q} \Gamma(v)$.

A *linear block code* is a subspace $\mathcal{C} \leq (\mathbb{F}_{q^m}^n, d_H)$ and a *rank metric code* is a subspace $\mathcal{C} \leq (\mathbb{F}_{q^m}^n, d_R)$, where $d_\Delta(v, w) = w_\Delta(v - w)$ for $\Delta \in \{H, R\}$.

# Support of codes

## Definition

Let $v \in \mathbb{F}_{q^m}^n$, and $V \subseteq \mathbb{F}_{q^m}^n$

- *Hamming support:*

$$S_H(v) := \{i : v_i \neq 0\} \quad \text{and} \quad S_H(V) := \bigcup_{v \in V} S_H(v)$$

- *rank support:*

$$S_R(v) := \operatorname{colsp}_{\mathbb{F}_q}(\Gamma(v)) \quad \text{and} \quad S_R(V) := \sum_{v \in V} S_R(v).$$

# Matroid/$q$-matroid

$$2^S := \{A : A \subseteq S\} \quad \mathcal{V}(\mathbb{F}_q^n) := \{V : V \leq \mathbb{F}_q^n\}.$$

## Definition

$M = (S, r)$ is a *matroid* if $r : 2^S \to \mathbb{N}$ satisfies:

(R1) $0 \leq r(A) \leq |A|$.

(R2) if $A \subseteq B$ then $r(A) \leq r(B)$.

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

$S$ is the *groundset* and $r$ the *rank function*

$\mathcal{M} = (\mathbb{F}_q^n, \rho)$ is a *q-matroid* if $\rho : \mathcal{V}(\mathbb{F}_q^n) \to \mathbb{N}$ satisfies:

(qR1) $0 \leq \rho(V) \leq \dim V$.

(qR2) if $V \leq W$ then $\rho(V) \leq \rho(W)$.

(qR3) $\rho(V + W) + \rho(V \cap W) \leq \rho(V) + \rho(W)$.

$\mathbb{F}_q^n$ is the *groundspace* and $\rho$ the *rank function*

## Example

$U_{k,n} = ([n], r)$ such that $r(A) = \min\{|A|, k\}$
$\mathcal{U}_{n,k} = (\mathbb{F}_q^n, \rho)$ such that $\rho(V) = \min\{\dim V, k\}$.

# ($q$-)Matroid arising from codes

$e_i \in \mathbb{F}_q^n$ is the $i^{th}$ standard basis vector.

For $V \leq \mathbb{F}_q^n$ let $Y_V \in \mathbb{F}_q^{n \times t}$ such that $\text{colsp}_{\mathbb{F}_q}(Y_V) = V$.

## Proposition

*Let $G \in \mathbb{F}_{q^m}^{k \times n}$ a generating matrix of $\mathcal{C} \leq \mathbb{F}_{q^m}^n$. Define $r : [n] \to \mathbb{N}_0$ and $\rho : \mathcal{L}(\mathbb{F}_q^n) \to \mathbb{N}_0$ such that:*

$$r(A) = rk_{\mathbb{F}_{q^m}} \left( G \cdot \begin{bmatrix} e_{i_1} & \cdots & e_{i_a} \end{bmatrix} \right) \text{ for all } A \subseteq [n]$$
$$\rho(V) = rk_{\mathbb{F}_{q^m}} \left( G \cdot Y_V \right) \text{ for all } V \leq \mathbb{F}_q^n.$$

*Then $M_{\mathcal{C}} := ([n], r)$ is a matroid and $\mathcal{M}_{\mathcal{C}} = (\mathbb{F}_q^n, \rho)$ is a $q$-matroid.*

## Definition

If a matroid $M$ (resp. $q$-matroid $\mathcal{M}$) arises from a code then $M$ (resp. $\mathcal{M}$) is *representable*.

# Example

## Example

Let $G \in \mathbb{F}_{2^5}^{3\times 4}$ where $\alpha^5 = \alpha^2 + 1$.

$$G = \begin{bmatrix} 1 & \alpha & \alpha^2 & \alpha^3 \\ 1 & \alpha^2 & \alpha^4 & \alpha^6 \\ 1 & \alpha^4 & \alpha^8 & \alpha^{12} \end{bmatrix}$$

- $M_{\mathcal{C}} = ([4], r) = U_{3,4}, \quad r(\{1,2\}) = \mathrm{rk}_{\mathbb{F}_{2^5}} \left( \begin{bmatrix} 1 & 1 & 1 \\ \alpha & \alpha^2 & \alpha^4 \end{bmatrix}^T \right) = 2$
- $\mathcal{M}_{\mathcal{C}} = (\mathbb{F}_2^4, \rho) = \mathcal{U}_{3,4}$

$$\rho(\langle (1100), (0010) \rangle) = \mathrm{rk}_{\mathbb{F}_{2^5}} \left( \begin{bmatrix} 1+\alpha & 1+\alpha^2 & 1+\alpha^4 \\ \alpha^2 & \alpha^4 & \alpha^8 \end{bmatrix}^T \right) = 2.$$

# More on ($q$-)matroids.

## Definition

$M = (S, r)$ is a matroid and $A \subseteq S$. The contraction of $A$ from $M$ is the matroid $M/A = (A^C, r')$ where $r'(B) = r(B \cup A) - r(A)$.

$\mathcal{M} = (\mathbb{F}_q^n, \rho)$ is a $q$-matroid and $V \subseteq \mathbb{F}_q^n$. The contraction of $V$ from $\mathcal{M}$ is the $q$-matroid $\mathcal{M}/V = (\mathbb{F}_q^n/V, \rho')$ where $\rho'(W/V) = r(W + V) - r(V)$.

## Definition

A flat of:

$M = (S, r)$ is $F \subseteq S$ s.t $r(F \cup e) > r(F)$ for all $e \notin F$.

$\mathcal{M} = (\mathbb{F}_q^n, \rho)$ is $F \leq \mathbb{F}_q^n$ s.t $\rho(F + \langle v \rangle) > \rho(F)$ for all $v \notin F$.

The collection of flat of $M$ and $\mathcal{M}$ is denoted by $\mathcal{F}_M$ and $\mathcal{F}_{\mathcal{M}}$.

## Proposition

*$\mathcal{F}_M$ and $\mathcal{F}_{\mathcal{M}}$ are geometric lattices.*

# The Characteristic polynomial

Throughout for $M = (S, r)$ and $\mathcal{M} = (\mathbb{F}_q^n, \rho)$ assume for all $e \in S$ and $v \in \mathbb{F}_q^n$ that $r(e) \neq 0 \neq \rho(v)$.

## Definition/Proposition (Whittle [2] - 1992)

The *characteristic polynomial*:

of a matroid $M = (S, r)$ with flats $\mathcal{F}_M$

$$\chi_M(x) := \sum_{A \subseteq S} (-1)^{|A|} x^{r(S)-r(A)} = \sum_{F \in \mathcal{F}_M} \mu_{\mathcal{F}_M}(0, F) x^{r(S)-r(F)}$$

of a $q$-matroid $\mathcal{M} = (\mathbb{F}_q^n, \rho)$ with flats $\mathcal{F}_\mathcal{M}$

$$\chi_\mathcal{M}(x) := \sum_{V \leq \mathbb{F}_q^n} (-1)^{\dim V} q^{\binom{\dim V}{2}} x^{\rho(\mathbb{F}_q^n)-\rho(V)} = \sum_{F \in \mathcal{F}_\mathcal{M}} \mu_{\mathcal{F}_\mathcal{M}}(0, F) x^{\rho(\mathbb{F}_q^n)-\rho(F)}$$

where $\mu_\mathcal{F}(\cdot, \cdot)$ is the Mobius function of the lattice $\mathcal{F}$.

# Remark on Characteristic Polynomial

The characteristic polynomial is an important object that captures many invariants of the code. One of the most celebrated result relating matroid theory and coding theory is the critical theorem.

**Theorem (Crapo, Rota [3] - 1970)**

*Let $\mathcal{C} \leq \mathbb{F}_{q^m}^n$ be a block code and $M = (S, r)$ its matroid. For all $A \subseteq S$*

$$|\{V = (v_1, \ldots, v_t) \,:\, v_i \in \mathcal{C} \text{ and } S_H(V) = A\}| = \chi_{M/A^C}(q^{mt})$$

# The projectivization matroid

Let $\mathbb{PF}_q^n := \{\langle v\rangle \,:\, v \in \mathbb{F}_q^n\}$

For $A \subseteq \mathbb{PF}_q^n$, let $\langle A\rangle := \left\langle \{v \in \mathbb{F}_q^n \,:\, \langle v\rangle \in A\}\right\rangle$

**Theorem (Johnsen, Pratihar, Verdure [4] - 2021)**

*Let $\mathcal{M} = (\mathbb{F}_q^n, \rho)$ be a q-matroid and let $r : 2^{\mathbb{PF}_q^n} \to \mathbb{N}$ such that for all $S \subseteq \mathbb{PF}_q^n$,*

$$r(S) = \rho(\langle S\rangle).$$

*Then $P(\mathcal{M}) := (\mathbb{PF}_q^n, r)$ is a matroid, and is called the projectivization matroid of $\mathcal{M}$.*

**Example**

Let $\mathcal{M} = (\mathbb{F}_2^3, \rho)$ such that $\rho(V) = \min\{\dim V, 2\}$ for all $V \leq \mathbb{F}_2^3$.
Consider $A = \{\langle(1,1,1)\rangle, \langle(1,0,1)\rangle, \langle(0,1,0)\rangle\}$. Then $r(A) = \rho(\langle A\rangle) = 2$.

# Flats of $q$-matroid and projectivization matroid

For $V \leq \mathbb{F}_q^n$, let $P(V) := \{\langle v \rangle : v \in V\}$.
$P(\mathcal{F}_{\mathcal{M}}) := \{P(F) : F \in \mathcal{F}_{\mathcal{M}}\}$

## Theorem (Johnsen et.al. [4] / J. [5] - 2022)

*$\mathcal{M}$ a $q$-matroid, $P(\mathcal{M})$ its projectivization matroid, and $\mathcal{F}_{\mathcal{M}}$, $\mathcal{F}_{P(\mathcal{M})}$ their respective lattice of flats. Then*

$$\mathcal{F}_{P(\mathcal{M})} = P(\mathcal{F}_{\mathcal{M}}),$$

*Furthermore for all $F \leq \mathcal{F}_{\mathcal{M}}$ then*

$$\mathcal{F}_{\mathcal{M}/F} \cong \mathcal{F}_{P(\mathcal{M})/P(F)}.$$

## Corollary (J. [5])

*Let $\mathcal{M}$ be a $q$-matroid, $P(\mathcal{M})$ its projectivization matroid and $W \leq \mathbb{F}_q^n$. Then*

$$\chi_{\mathcal{M}/W}(x) = \chi_{P(\mathcal{M})/P(W)}(x).$$

# Hamming-metric code associated to rank metric code

## Definition (Alfarano, Borello, Neri, Ravagnani [6] - 2021)

Let $\mathcal{C} \leq \mathbb{F}_{q^m}^n$ be a rank metric code and $G \in \mathbb{F}_{q^m}^{k \times n}$ such that $\mathrm{rowsp}_{\mathbb{F}_{q^m}}(G) = \mathcal{C}$.

Let $H \in \mathbb{F}_q^{n \times \frac{q^n-1}{q-1}}$ where each column of $H$ is a representative of a distinct element of $\mathbb{PF}_q^n$.

The code $\mathcal{C}^H := \{vH : v \in \mathcal{C}\} = \mathrm{rowsp}_{\mathbb{F}_{q^m}}(G \cdot H)$ is called a *Hamming-metric code associated to $\mathcal{C}$ via $H$*.

## Example

$G = \begin{bmatrix} 1 & 0 & \alpha \\ 0 & 1 & \alpha+1 \end{bmatrix} \in \mathbb{F}_{2^2}^3$ and $H = \begin{bmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix} \in \mathbb{F}_2^{3 \times 7}$. Then

$G^H = \begin{bmatrix} 1 & 0 & & \alpha & 1 & 1+\alpha & \alpha & 1+\alpha \\ 0 & 1 & \alpha+1 & 1 & \alpha+1 & \alpha & \alpha & \end{bmatrix}$ and $\mathcal{C}^H := \mathrm{rowsp}_{\mathbb{F}_4}(G^H)$ is the Hamming metric code associated to $\mathcal{C} := \mathrm{rowsp}_{\mathbb{F}_4}(G)$.

# Representable projectivization matroid

**Theorem (J. [5])**

*Let $\mathcal{C} \leq \mathbb{F}_{q^m}^n$ be a rank metric code, $\mathcal{M}_{\mathcal{C}}$ its q-matroid, and $P(\mathcal{M}_{\mathcal{C}})$ its projectivization matroid.*

*Let $\mathcal{C}^H$ be a Hamming-metric code associated to $\mathcal{C}$ via $H$ and $M_{\mathcal{C}^H}$ its matroid. Then*

$$P(\mathcal{M}_{\mathcal{C}}) \cong M_{\mathcal{C}^H} \quad \text{as matroids.}$$

**Corollary (J. [5])**

*If $\mathcal{M}$ is representable then so is $P(\mathcal{M})$.*

# Support of Hamming metric code associate to $\mathcal{C}$ via $H$

Let $\mathcal{C} \leq \mathbb{F}_{q^m}^n$ a rank metric code and $\mathcal{C}^H = \mathcal{C} \cdot H$ its associated Hamming-metric code via $H$.

Relabel coordinates of $\mathcal{C}^H$: $i \mapsto \langle h_i \rangle_{\mathbb{F}_q}$ where $h_i$ is the $i^{\text{th}}$ column of $H$.

## Proposition (J. [5])

*For all $V \subseteq \mathcal{C}$:*

$$S_R(V) = W \Leftrightarrow S_H(V \cdot H) = \mathbb{PF}_q^n - P(W^\perp)$$

*where $V \cdot H := \{v \cdot H \ : \ v \in V\}$*

# A $q$-analogue of the Critical Theorem

**Theorem (J. [5] / Alfarano, Byrne )**

*Let $\mathcal{C} \leq \mathbb{F}_{q^m}^n$ be a rank metric code and $\mathcal{M}$ its q-matroid. For all $W \leq \mathbb{F}_q^n$,*

$$|\{V = (v_1, \ldots, v_t) \,:\, v_j \in \mathcal{C} \text{ and } S_R(V) = W\}| = \chi_{\mathcal{M}/W^\perp}(q^{mt})$$

Sketch of proof:

- Since $\mathcal{M}$ is representable then so is $P(\mathcal{M})$. Apply Critical theorem to $P(\mathcal{M})$ and $\mathcal{C}^H = \{v \cdot H \,:\, v \in \mathcal{C}\}$.

  $$|\{V \cdot H = (v_1 \cdot H, \ldots, v_t \cdot H) \,:\, v_i \cdot H \in \mathcal{C}^H \text{ and } S_H(V) = P(W^\perp)^C\}| = \chi_{M/P(W^\perp)}(q^{mt})$$

- Use $S_R(V) = W \Leftrightarrow S_H(V \cdot H) = \mathbb{PF}_q^n - P(W^\perp)$.
- Use $\chi_{\mathcal{M}/W^\perp}(x) = \chi_{P(\mathcal{M})/P(W^\perp)}(x)$.

# Conclusion

- This proof shows the Critical Theorem for $q$-matroids can be seen to be a specific case of the Critical Theorem for matroids.
- The Critical problem for $q$-matroid is a specific case of the Critical problem for matroids.
- The characteristic polynomial of the projectivization matroid can be used to determined a deletion-contraction formula for the characteristic polynomial of $q$-matroids.

# References I


R. Jurrius and R. Pellikaan.

Defining the q-analogue of a matroid.

*Electronic Journal of Combinatorics*, 25, 10 2016.

G. Whittle.

*Characteristic polynomials of weighted lattices*.

Mathematics Department, Victoria University of Wellington, 1992.

H. Crapo and G-C. Rota.

*On the foundations of combinatorial theory: Combinatorial geometries*.

MIT press Cambridge, Mass., 1970.

T. Johnsen, R. Pratihar, and H. Verdure.

Weight spectra of gabidulin rank-metric codes and betti numbers.

*arXiv:2106.10993v3*, 2021.

# References II


B. Jany.

The projectivization matroid of a $q$-matroid.

*arXiv preprint arXiv:2204.01232*, 2022.

G.N. Alfarano, M. Borello, A. Neri, and A. Ravagnani.

Linear cutting blocking sets and minimal codes in the rank metric.

*arXiv preprint arXiv:2106.12465*, 2021.