q-Matroids, Cyclic Flats, and their Relations to Codes

Eimear Byrne
University College Dublin

(joint work with Gianira Alfarano)

Feb 20-24, 2023

ALCOCRYPT

Matroids

Definition

A **matroid** is a pair (S, r) satisfying

- S is a finite set; 2^E is the lattice of subsets of S
- $r : 2^S \to \mathbb{N}_0$ is a **rank function**, s.t. for all $A, B \in S$:
  - (r1) $0 \leq r(A) \leq |A|$.
  - (r2) If $A \subseteq B$ then $r(A) \leq r(B)$ (increasing).
  - (r3) $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$ (semimodularity).

Example

C is an $\mathbb{F}_q$-$[n, k]$ code with generator matrix $G = [G^1 | \cdots | G^n]$.

$C(S) := \{(c_s : s \in S) : c \in C\}$.

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

Then $M = M[C] := (2^{[n]}, r)$ is a matroid and is called **representable** (in $\mathbb{F}_q^k$).

Matroids

- A lot of matroid theory is inspired by graph theory and linear algebra.
- Many examples, constructions, and families come from graphs and codes.
- However, 'most' matroids are not representable (i.e. from codes).
  The proportion of representable matroids on $[n]$ tends to 0 as $n \longrightarrow \infty$ (Nelson, 2016).
- There are numerous axiomatic descriptions of matroids.
- Matroids arise in applications, e.g. secret sharing schemes, network coding, batch codes.

H. Whitney, "On the Abstract Properties of Linear Dependence", American J. Math., 57 (3), 1935.

Complemented Lattices

Boolean lattice	$\longrightarrow$	*Subspace Lattice*
$(2^E, \cup, \cap)$		$(\mathscr{L}(E), +, \cap)$
$\mu(0,x) = (-1)^{\lvert x \rvert}$		$\mu(0,U) = (-1)^{\dim(U)} q^{\binom{\dim(U)}{2}}$
Matroid	$\longrightarrow$	*q-Matroid*
Polymatroid	$\longrightarrow$	*q-Polymatroid*

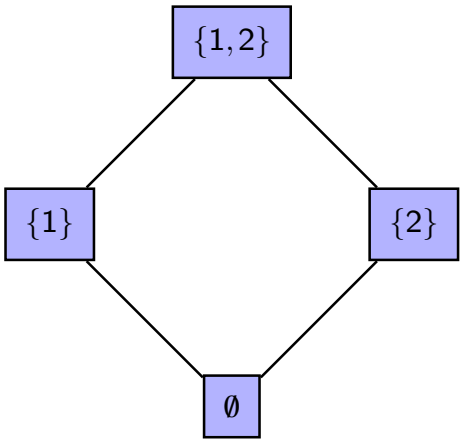


Figure: $\mathscr{L}(\{1,2\})$

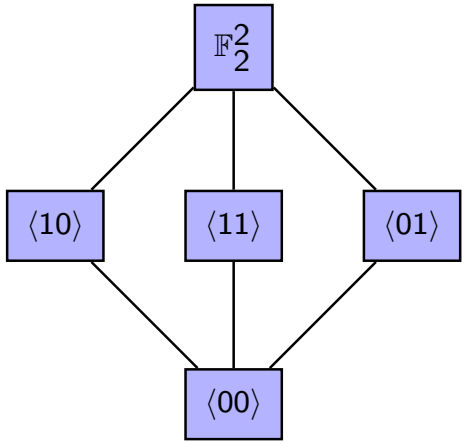


Figure: $\mathscr{L}(\mathbb{F}_2^2)$

Matroids $\longrightarrow$ q-Matroids

Definition

A **matroid** is a pair (S, r) satisfying

- S is a finite set; 2^S is the lattice of subsets of S
- $r : 2^S \to \mathbb{N}_0$ is a **rank function**, s.t. for all $A, B \in S$:

(r1) $0 \leq r(A) \leq |A|$ (bounded).
(r2) If $A \subseteq B$ then $r(A) \leq r(B)$ (increasing).
(r3) $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$ (semimodular).

Definition (Jurrius, Pellikaan, 2018)

A q-**matroid** is a pair (E, r) satisfying

- E is a finite dim'l vector space; $\mathscr{L}(E)$ is the lattice of subspaces of E
- $r : \mathscr{L}(E) \to \mathbb{N}_0$ is a **rank function**, s.t. for all $A, B \leq E$:

(R1) $0 \leq r(A) \leq \dim A$ (bounded).
(R2) If $A \leq B$ then $r(A) \leq r(B)$ (increasing).
(R3) $r(A + B) + r(A \cap B) \leq r(A) + r(B)$ (semimodular).

Rank-Metric Codes and q-Matroids

One well-known construction of a q-matroid arises from an $\mathbb{F}_{q^m}$-linear code C.
Let G be a $k \times n$ generator matrix over $\mathbb{F}_{q^m}$.
For every $U \in \mathscr{L}(\mathbb{F}_q^n)$, let A^U be a matrix whose columns form a basis of U.
Then the map

$$r : \mathscr{L}(\mathbb{F}_q^n) \to \mathbb{Z}, \ U \mapsto \mathrm{rk}(GA^U), \tag{1}$$

is the rank function of the q-matroid, $M[C] = (\mathbb{F}_q^n, r)$.

Example

Let $\alpha^3 = \alpha + 1$ in $\mathbb{F}_8$.

$$G := \begin{pmatrix} 1 & \alpha & \alpha^2 & 1 \\ 0 & 1 & \alpha & 0 \end{pmatrix} \in \mathbb{F}_8^{2\times 4}.$$

$M[C] = (\mathbb{F}_2^4, r)$.
$r(\langle e_2, e_3 \rangle) = \mathrm{rk}(G[e_2, e_3]) = 1$.
$r(\langle e_2 \rangle) = r(\langle e_3 \rangle) = r(\langle e_2 + e_3 \rangle) = 1$.
$r(\langle e_1 + e_2, e_3, e_4 \rangle) = \mathrm{rk}(G[e_1 + e_2, e_3, e_4]) = 2$.

Flats/Closed Spaces

Definition

A space $A \leq E$ is called a **flat** or **closed space** of a q-matroid $M = (E, r)$ if for all $x \leq E$ such that $x \not\leq A$, we have

$$r(A + x) > r(A).$$

We define:

$$\mathscr{F}_r := \{A \in \mathscr{L}(E) \mid r(A + x) > r(A)\ \forall x \leq E,\ x \not\leq A\}.$$

$\mathrm{cl}(A) :=$ minimal closed subspace containing A.

$\mathscr{F}_r$ forms a lattice with $F_1 \vee F_2 := \mathrm{cl}(F_1 + F_2)$ and $F_1 \wedge F_2 := F_1 \cap F_2$.

Example

$$G := \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha \\ 0 & 1 & \alpha & 1 \end{pmatrix} \in \mathbb{F}_8^{2\times 4}.$$

$r(\langle e_2, e_3, e_4\rangle) = \mathrm{rk}(G[e_2, e_3, e_4]) = 1. \forall v \in \mathbb{F}_2^4 \backslash \langle e_2, e_3, e_4\rangle, r(\langle v, e_2, e_3\rangle) = 2.$

$r(\langle e_1 + e_2, e_3, e_4\rangle) = 2 \implies \langle e_1 + e_2, e_3, e_4\rangle \notin \mathscr{F}_r.$

Cyclic/Open Spaces

Definition

A space $A \leq E$ is called a **cyclic space** or an **open space** of a q-matroid $M = (E, r)$ if

$$\mathrm{cl}(A) = \mathrm{cl}(B)$$

for every $B \in \mathrm{Hyp}(A)$:=hyperplanes of A. We define:

$$\mathscr{C}_r := \{A \in \mathscr{L}(E) \mid r(A) = r(B)\ \forall B \in \mathrm{Hyp}(A)\}.$$

$\mathrm{cyc}(A) :=$ maximal open subspace contained in A.

$\mathscr{C}_r$ forms a lattice with $C_1 \vee C_2 := C_1 + C_2$ and $C_1 \wedge C_2 := \mathrm{cyc}(C_1 \cap C_2)$.

Example

$$G := \begin{pmatrix} 1 & \alpha & \alpha^2 & 1 \\ 0 & 1 & \alpha & 0 \end{pmatrix} \in \mathbb{F}_8^{2\times 4}.$$

$r(\langle e_2, e_3\rangle) = r(\langle e_2\rangle) = r(\langle e_3\rangle) = r(\langle e_2 + e_3\rangle) = 1 \implies \langle e_2, e_3\rangle \in \mathscr{C}_r.$

$r(\langle e_1 + e_2, e_3, e_4\rangle) = 2, \mathrm{cyc}(\langle e_1 + e_2, e_3, e_4\rangle) = \langle e_1 + e_2 + e_4, e_3\rangle.$

For any $c \in \mathbb{F}_{q^m}^n$,

$$\sigma(c) := \text{colsp}(\hat{c}),$$

where $\hat{c}$ is the $n \times m$ matrix representation of c over $\mathbb{F}_q$.

Theorem (Alfarano, B. '22)

Let $c \in C^\perp$. Then

1. *$\sigma(c)$ is a cyclic space in $M[C]$ and*
2. *c is minimal in $C^\perp$ if c is a circuit.*

The cyclic spaces of the q-matroid $M[C]$ are the supports of codewords in $C^\perp$.

The minimal dependent spaces of $M[C]$ are the supports of minimal codewords of $C^\perp$.

The Dual q-Matroid

Let $M = (E, r)$ be a q-matroid. For each $A \leq E$, define:

$$r^*(A) := \dim(A) - r(E) + r(A^\perp).$$

$M^* = (E, r^*)$ is a q-matroid called the **dual** of M.

- $M^{**} = M$.
- $M[C]^* \cong M[C^\perp]$ [Gorla+, 2019].

Lemma (Johnsen+, '22)

$A \leq E$ is cyclic in M if and only if $A^\perp$ is a flat of M^*.

E. Gorla, R. Jurrius, H. López, A. Ravagnani, 'Rank-metric codes and q-polymatroids,' J. Alg. Comb., 2019.

T. Johnsen, R. Pratihar, and H. Verdure, 'Weight Spectra of Gabidulin Rank-Metric Codes and Betti Numbers,' Sao Paulo J. Math. Sc., 2022.

Flat Axioms

Definition

Let $\mathscr{F} \subseteq \mathscr{L}(E)$. We define the following **flat axioms**.

(F1) $E \in \mathscr{F}$.

(F2) If $F_1 \in \mathscr{F}$ and $F_2 \in \mathscr{F}$, then $F_1 \cap F_2 \in \mathscr{F}$.

(F3) For all $F \in \mathscr{F}$ and $x \leq E$, $x \not\leq F$, there is a unique cover of F in $\mathscr{F}$ that contains x.

If satisfies the flat axioms (F1)-(F3) we say that $(E, \mathscr{F})$ is a collection of **flats**.

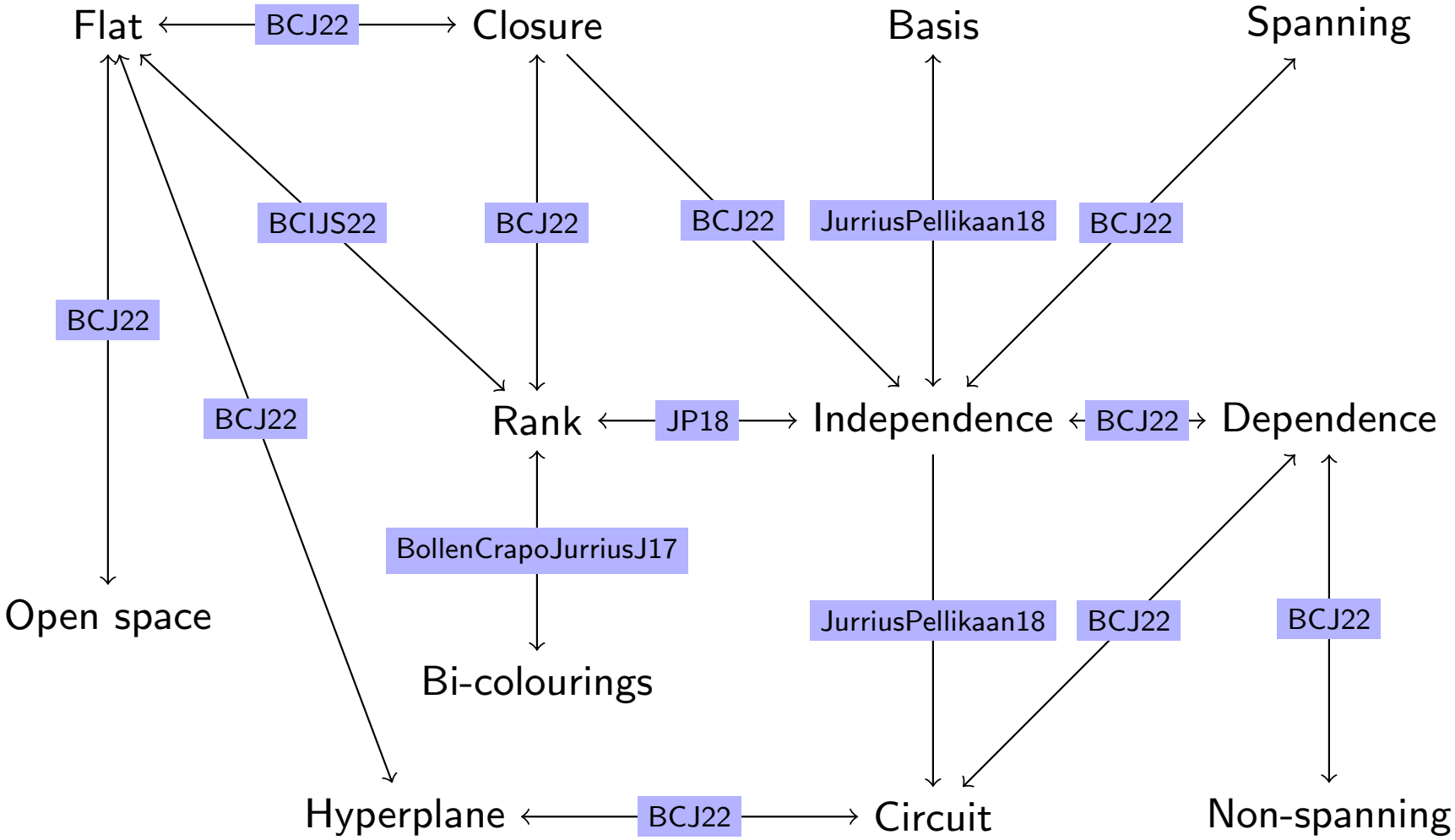
Theorem (B.+, '22)

Let $\mathscr{F}$ be a collection of flats and let $r_{\mathscr{F}}(A) := \min$ length of a chain of flats in A.
Then $(E, r_{\mathscr{F}})$ is a q-matroid with lattice of flats $\mathscr{F}_{r_{\mathscr{F}}} = \mathscr{F}$.
Conversely, if (E, r) is a q-matroid, then $\mathscr{F}_r$ is lattice of flats and $r = r_{\mathscr{F}_r}$.

The lattice of flats of M determines the q-matroid M.

E. Byrne E, M. Ceria, S. Ionica, R. Jurrius, E. Saçıkara, 'Constructions of new Matroids and Designs over $\mathbb{F}_q$,' Designs, Codes, and Cryptography, 2022.

Cryptomorphisms



E. Byrne, M. Ceria, R. Jurrius, 'Constructions of New Cryptomorphisms,' J. Comb. Th. (B), 2022.

Lattice of Cyclic Flats

A cyclic flat is a flat that is cyclic!

Lemma

The set $\mathscr{Z}_r$ of cyclic flats of a q-matroid $M = (E, r)$ forms a lattice under inclusion, where for any $F_1, F_2 \in \mathscr{Z}_r$:

$$F_1 \wedge F_2 := \mathrm{cyc}(F_1 \cap F_2) \text{ and } F_1 \vee F_2 := \mathrm{cl}(F_1 + F_2).$$

Theorem (Alfarano, B., '22)

A q-matroid $M = (E, r)$ is uniquely determined by its lattice of cyclic flats along with their ranks.

This can be shown by an algorithm[1] that reconstructs the lattice of flats $\mathscr{F}_r$ using knowledge of $\mathscr{Z}_r$ along with the ranks of its elements.

[1] R. Freij-Hollanti, M. Grezet, C. Hollanti, T. Westerbäck. 'Cyclic flats of binary matroids.' Adv. Appl. Math., 2021.

Cyclic Flats

- A q-matroid is completely determined by its (ranked) lattice of cyclic flats.
- Cyclic flats play an important role in defining invariants, such as the Tutte polynomial of a (q)-matroid.
- Cyclic flats are important in the theory of transversal matroids.
- The lattice of cyclic flats of a (q)-matroid is small compared to the lattice of flats or the lattice of cycles.

Lattice of Cyclic Flats

Example

Let C have generator matrix:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & \alpha & \alpha^2 \end{pmatrix} \in \mathbb{F}_2^{2\times 4}.$$

The only cyclic flats of $M[C]$ are $\langle 0 \rangle$ and $\langle e_2, e_3, e_4 \rangle$.

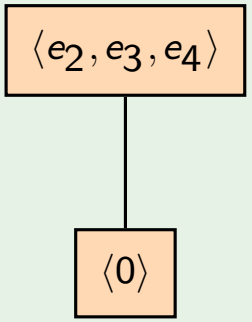


Figure: Lattice of cyclic flats of the matroid $M[C]$

Lattice of Flats

Example

Let C have generator matrix:

$$G = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & \alpha & \alpha^2 \end{pmatrix} \in \mathbb{F}_2^{2\times 4}.$$

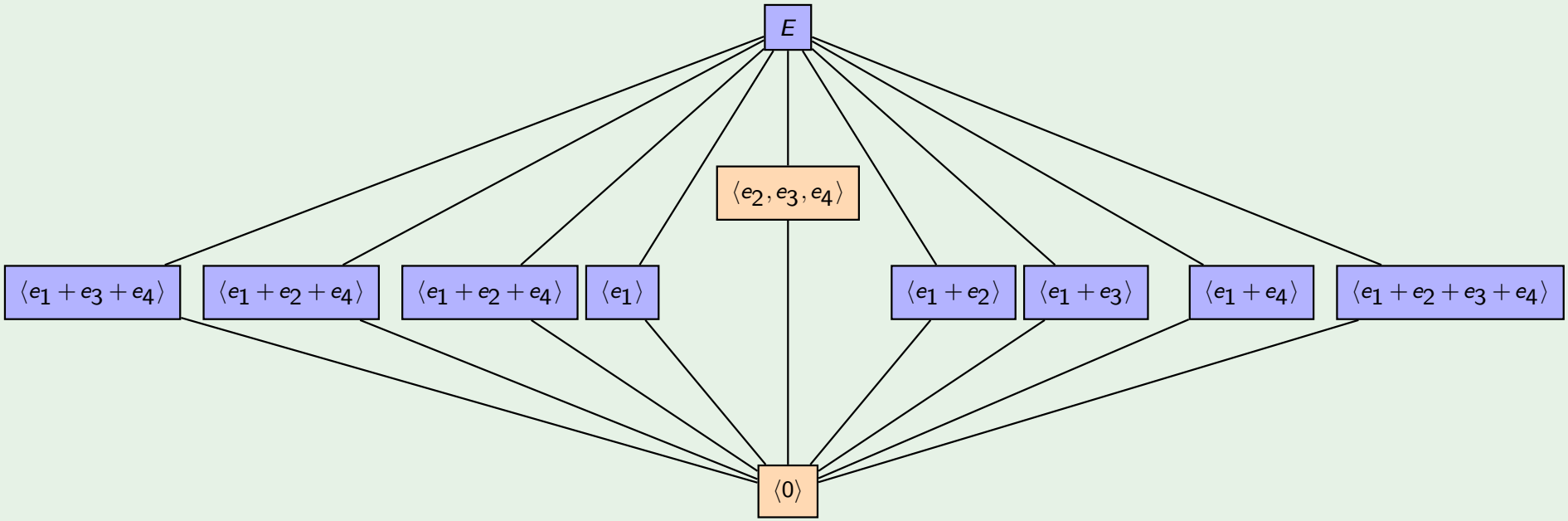


Figure: Lattice of flats of the matroid $M[C]$

Cyclic Flat Axioms

Definition

Let $\mathscr{Z} \subset \mathscr{L}(E)$ and let $(\mathscr{Z}, \leq, \vee, \wedge)$ be a lattice s.t. $\forall Z_1, Z_2 \in \mathscr{Z}$,

$$Z_1 + Z_2 \leq Z_1 \vee Z_2 \text{ and } Z_1 \wedge Z_2 \leq Z_1 \cap Z_2.$$

Let $f : \mathscr{Z} \to \mathbb{Z}$ be a map. We define the following **cyclic flat** axioms.

(Z1) $f(0_{\mathscr{Z}}) = 0$, where $0_{\mathscr{Z}}$ is the minimal element of $\mathscr{Z}$.

(Z2) For every $F, G \in \mathscr{Z}$ such that $G \lneq F$, we have:

$$0 < f(F) - f(G) < \dim(F) - \dim(G).$$

(Z3) For every $F, G \in \mathscr{Z}$ we have:

$$f(F) + f(G) \geq f(F \vee G) + f(F \wedge G) + \dim((F \cap G)/(F \wedge G)).$$

If $(\mathscr{Z}, f)$ satisfies the cyclic flat axioms, we say that $\mathscr{Z}$ is a lattice of **cyclic flats** wrt f.

The Cyclic Flats of a q-Matroid are Cyclic Flats!!

Theorem (Alfarano, B., '22)

Let $M = (E, r)$ be a q-matroid and let $f : \mathscr{Z}_r \to \mathbb{Z}$, be the map defined by

$$f(F) = r(F) \; \forall \; F \in \mathscr{Z}_r.$$

Then $(\mathscr{Z}_r, f)$ satisfies (Z1)–(Z3).

What about the converse?

Does a collection of cyclic flats determine a q-matroid?

A Convolution and Cryptomorphism

Definition

Let $\mathscr{Z} \subseteq \mathscr{L}(E)$. For every map $f : \mathscr{L}(E) \longrightarrow \mathbb{N}_0$, define $f_{\mathscr{Z}} : \mathscr{L}(E) \longrightarrow \mathbb{N}_0$ by:

$$f_{\mathscr{Z}}(A) := \min\{f(F) + \dim((A+F)/F) \mid F \in \mathscr{Z}\}, \text{ for all } A \in \mathscr{L}(E).$$

Theorem (Alfarano, B., '22)

Let $(\mathscr{Z}, f)$ be a lattice of cyclic flats (i.e., it satisfies (Z1)-(Z3)).
Then

1. *$f_{\mathscr{Z}}$ satisfies the axioms (R1)–(R3), i.e., $(E, f_{\mathscr{Z}})$ is a q-matroid and*
2. *$\mathscr{Z} = \mathscr{Z}_{f_{\mathscr{Z}}}$.*

So, if we have a lattice $\mathscr{Z}$ satisfying (Z1)–(Z3) then it determines a q-matroid whose collection of cyclic flats is $\mathscr{Z}$.

A space $I \leq E$ is independent in $M = (E, r)$ if $r(I) = \dim(I)$.

Theorem (Alfarano, B. '22)

Let $G \in \mathbb{F}_{q^m}^{k \times n}$ be a generator matrix of C and let $\mathscr{U}$ be the n-dim'l $\mathbb{F}_q$-span of the columns of G.
Let

$$\psi_G : \mathbb{F}_q^n \to \mathscr{U}, \ v \mapsto vG^\top.$$

Let $M[C] = (E, r)$ and let $\mathscr{I}_r$ be the independent spaces of $M[C]$.
Let

$$\mathscr{I} := \{V \leq \mathscr{U} \mid \dim_{\mathbb{F}_{q^m}}(V \otimes_{\mathbb{F}_q} \mathbb{F}_{q^m}) = \dim_{\mathbb{F}_q}(V)\}.$$

Then

1. $(\mathscr{U}, \mathscr{I})$ *is a q-matroid and*
2. $\{\psi_G(I) \leq \mathscr{U} \mid I \in \mathscr{I}_r\} = \mathscr{I}$.

So, the independent spaces of $M[G]$ are those corresponding to columns of G that have the same rank over $\mathbb{F}_q$ or $\mathbb{F}_{q^m}$.

Thank you!

- Byrne, Ceria, Jurrius, 'Constructions of New Cryptomorphisms,' Journal of Combinatorial Theory, Series B 153, 149-194, 2022.
- J. E. Bonin and A. De Mier, 'The lattice of cyclic flats of a matroid,' Ann. Comb., 12(2):155–170, 2008.
- R. Freij-Hollanti, M. Grezet, C. Hollanti, and T. Westerbäck. Cyclic flats of binary matroids. Adv. Appl. Math., 127:102165, 2021.
- T. Johnsen, R. Pratihar, and H. Verdure, 'Weight spectra of Gabidulin rank-metric codes and Betti numbers,' Sao Paulo Journal of Mathematical Sciences, 2022.
- Gorla, Jurrius, Löpez, Ravagnani. 'Rank-metric codes and q-polymatroids,' Journal of Algebraic Combinatorics, 2019.
- Jurrius, Pellikaan, 'Defining the q-analogue of a matroid,' Electronic Journal of Combinatorics, 25(3), 2018.
- Shiromoto, 'Codes with the rank metric and matroids,' Designs, Codes and Cryptography, 87(8), 2019.