q-Matroids and their Cryptomorphisms

Eimear Byrne
University College Dublin

June 3, 2021

Women in Combinatorics Virtual Colloquium

q-Analogues

q-Analogues

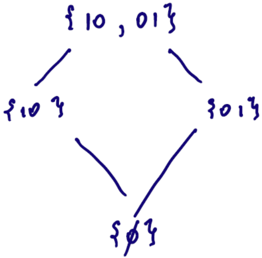
subsets $\{s_1, \ldots, s_k\}$ *of* $[n]$	*subspaces* $\langle s_1, \ldots, s_k \rangle$ *of* $\mathbb{F}^n$
set cardinality: $\vert S\vert$	*vector space dimension:* $\dim(S)$
set complement: $[n] - S$	*orthogonal complement:* $S^\perp$
binomial coefficients $\binom{n}{k}$	*Gaussian coefficients* $\begin{bmatrix} n \\ k \end{bmatrix}_q$
Hamming weight of $(v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n$	$\mathbb{F}_q$*-dimension of* $(v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n$
Hamming weight of $(v_1, \ldots, v_n) \in \mathbb{F}_{q^m}^n$	$\mathbb{F}_q$*-rank of* $\begin{pmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ v_{m1} & v_{m2} & \cdots & v_{mn} \end{pmatrix} \in \mathbb{F}_q^{m \times n}$

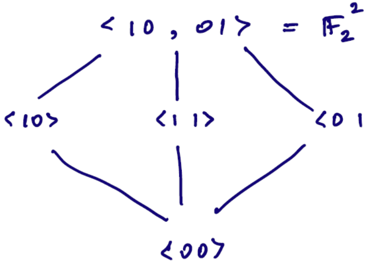
$$1 \longleftarrow q$$

q-Analogues in Coding Theory

Block codes - subspaces of $\mathbb{F}_q^n$	$\longrightarrow$	*Matrix codes - subspaces of* $\mathbb{F}_q^{n\times m}$
Reed-Solomon Codes	$\longrightarrow$	*Delsarte-Gabidulin Codes*
Hamming metric	$\longrightarrow$	*Rank metric*
$d_H(x,y) = \|\{i : x_i \neq y_i\}\|$		$\mathrm{rk}(X - Y)$
Row space of a matrix	$\longrightarrow$	*Slice space of a 3-tensor*
MDS codes	$\longrightarrow$	*MRD codes*

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*





Matroids

Matroids

- Matroids are objects that generalize concepts in **graph theory** and **linear algebra**.
- Graphs: circuits, cycles, dual, contraction, deletion
- Linear algebra: independence, bases, flats, closure, rank
- Applications: information theory, secret sharing, distributed storage, coding theory, combinatorial optimization
- A matroid can be characterized as finite geometric lattice (its lattice of flats).
- In fact a matroid can be equivalently determined by its flats, independent sets, bases, hyperplanes, circuits, closure function, rank function etc.
- These equivalent descriptions of a matroid are called **cryptomorphisms**.
- Have a lot of different cryptomorphisms can be quite useful for defining and characterizing matroids.

Definition

A **matroid** is a pair (E, r) satisfying the following.

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

Matroids and Rank Functions

Definition

A **matroid** is a pair (E, r) satisfying the following.

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

Example

Let k be a positive integer, $k \leq n$. $U_{k,n}$ is the uniform matroid, with rank function:

$$r(U) := \begin{cases} |U| & \text{if } |U| \leq k, \\ k & \text{if } |U| > k. \end{cases}$$

Matroids and Rank Functions

Definition

A **matroid** is a pair (E, r) satisfying the following.

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

Example

Let k be a positive integer, $k \leq n$. $U_{k,n}$ is the uniform matroid, with rank function:

$$r(U) := \begin{cases} |U| & \text{if } |U| \leq k, \\ k & \text{if } |U| > k. \end{cases}$$

(r3) If $|A \cup B| \leq k$ then $r(A \cup B) + r(A \cap B) = |A \cup B| + |A \cap B| = |A| + |B| = r(A) + r(B)$.
If $|A| > k$ then $r(A \cup B) + r(A \cap B) = k + r(A \cap B) \leq k + r(B) = r(A) + r(B)$.
Etc

Definition

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

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

Example

Let $E = \{1, \ldots, 5\}$. Let $A = \begin{bmatrix} 1 & 0 & 2 & 1 & 0 \\ 0 & 1 & 2 & 1 & 2 \end{bmatrix} \in \mathbb{F}_3^{2\times 5}$.

Define $r(S) = \dim(\langle \mathrm{col}(A, s) : s \in S \rangle)$.

Each singleton has rank 1. $r(\{2,5\}) = r(\{3,4\}) = 1$, $r(S) = 2$ for all other subsets.

We say that $\{2,5\}$ and $\{3,4\}$ are **dependent sets**.

Flats, Circuits & Independent Spaces of a Matroid

Definition

Let $M=(E,r)$ be a matroid. Let $A\subseteq E$. A is called:

1. a **flat** if $r(A\cup\{x\})>r(A)$ $x\leq E, x\nleq A$,
2. **independent** if $r(A)=|A|$,
3. **dependent** if it is not independent,
4. a **circuit** if it is dependent and every proper subset of A is independent.
5. The **closure** of A is $\mathrm{cl}(A):=\{x\in E : r(A\cup\{x\})=r(A)\}$.

Flats, Circuits & Independent Spaces of a Matroid

Definition

Let $M = (E, r)$ be a matroid. Let $A \subseteq E$. A is called:

1. a **flat** if $r(A \cup \{x\}) > r(A)$ $x \leq E, x \not\leq A$,
2. **independent** if $r(A) = |A|$,
3. **dependent** if it is not independent,
4. a **circuit** if it is dependent and every proper subset of A is independent.
5. The **closure** of A is $\mathrm{cl}(A) := \{x \in E : r(A \cup \{x\}) = r(A)\}$.

Example

Let k be a positive integer, $k \leq n$. $U_{k,n}$ is the uniform matroid, with rank function:

$$r(U) := \begin{cases} |U| & \text{if } |U| \leq k, \\ k & \text{if } |U| > k. \end{cases}$$

- A is independent if $|A| \leq k$.
- A is a circuit if $|A| = k + 1$.
- A is a flat if $|A| \leq k - 1$ or if $A = E$.

There are separate axiom systems that equivalently defines a matroid.

- independence (i1)-(i3),
- flats (f1)-(f3),
- circuits (c1)-(c3),
- closure (cl1)-(cl4),
- Etc

(Independence Axioms)

Let $\mathscr{I} \subseteq 2^E$. $\mathscr{I}$ is a collection of independent sets if it satisfies the following.

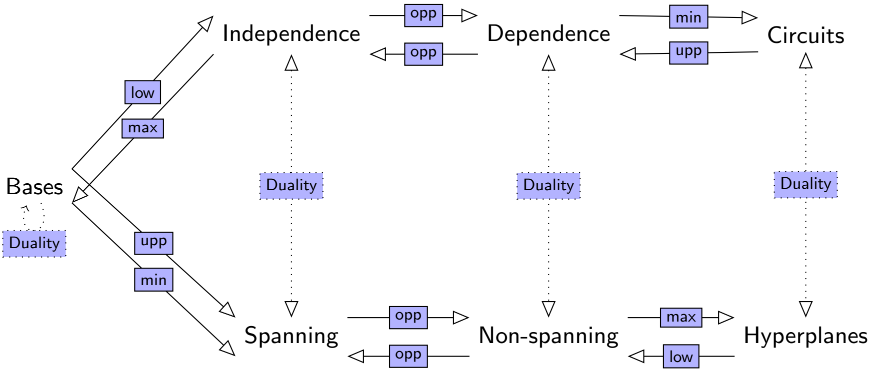
(i1) $\emptyset \in \mathscr{I}$.

(i2) *If $I \subseteq J$ and $J \in \mathscr{I} \implies I \in \mathscr{I}$ (decreasing).*

(i3) *If $I, J \in \mathscr{I}$ and $|I| \leq |J|$ then $\exists\, x \in J$ s.t $\{x\} \cup I \in \mathscr{I}$ (augmentation).*

For example, if $\mathscr{I}$ is a collection of independent spaces, then it defines a matroid (E, r) whose set of independent sets is $\mathscr{I}$. Conversely, if (E, r) is a matroid, its set of independent sets satisfies $(i1) - (i3)$.

Cryptomorphisms with Duality



q-Matroids

Definition

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

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

Definition

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

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

Definition

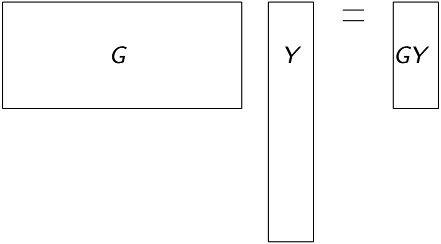
A q-**matroid** is a pair (E, r) satisfying

- 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) $0 \leq r(A) \leq \dim A$.
  (R2) If $A \leq B$ then $r(A) \leq r(B)$.
  (R3) $r(A + B) + r(A \cap B) \leq r(A) + r(B)$ (semimodularity).

Representable q-Matroids

Every $\mathbb{F}_{q^m}$-linear **rank metric code** *gives a q-matroid. [Jurrius, Pellikaan, 2018]*

Let $E = \mathbb{F}_q^n$ and let G be a $k \times n$ matrix of rank k over $\mathbb{F}_{q^m}$.
Let $A \subseteq E$ and Y a matrix whose columns span A.



Then $r(A) = \mathrm{rk}(GY)$ satisfies the axioms (R1), (R2), (R3).

This is a **representable** q-matroid.

Matrix codes for the rank metric give q-**polymatroids**.

Flats, Circuits, Closure & Independent Spaces of a q-Matroid

Definition

Let $M = (E, r)$ be a q-matroid. Let $A \leq E$. A is called:

1. a **flat** if $r(A + x) > r(A)$ $x \leq E, x \not\leq A$,
2. **independent** if $r(A) = \dim A$,
3. **dependent** if it is not independent,
4. a **circuit** if it is dependent and every proper subspace of A is independent.
5. The **closure** of A is $\mathrm{cl}(A) := \max\{F \leq E : A \leq F, r(A + F) = r(A)\}$.

Flats, Circuits, Closure & Independent Spaces of a q-Matroid

Definition

Let $M=(E,r)$ be a q-matroid. Let $A \leq E$. A is called:

1. a **flat** if $r(A+x) > r(A)$ $x \leq E, x \not\leq A$,
2. **independent** if $r(A) = \dim A$,
3. **dependent** if it is not independent,
4. a **circuit** if it is dependent and every proper subspace of A is independent.
5. The **closure** of A is $\mathrm{cl}(A) := \max\{F \leq E : A \leq F, r(A+F) = r(A)\}$.

Example

Let k be a positive integer, $k \leq n$. $U_{k,n}$ is the uniform q-matroid, with rank function:

$$r(U) := \begin{cases} \dim(U) & \text{if } \dim(U) \leq k, \\ k & \text{if } \dim(U) > k. \end{cases}$$

- A is independent if $\dim(A) \leq k$.
- A is a circuit if $\dim(A) = k+1$.
- A is a flat if $\dim(A) \leq k-1$ or if $A = E$.

Axioms

Independence Axioms

Independent Sets	*Independent Spaces*
(i1) $\emptyset \in \mathscr{I}$.	*(I1)* $0 \in \mathscr{I}$.
(i2) If $I \subseteq J, J \in \mathscr{I} \implies I \in \mathscr{I}$.	*(I2) If* $I \leq J, J \in \mathscr{I} \implies I \in \mathscr{I}$.
(i3) If $I, J \in \mathscr{I}$, $\vert I\vert < \vert J\vert$ *then*	*(I3) If* $I, J \in \mathscr{I}$, $\dim(I) < \dim(J)$ *then*
$\exists\, x \in J \backslash I$ *s.t.* $\{x\} \cup I \in \mathscr{I}$.	$\exists\, x \leq J, x \not\leq I$, $\dim(x) = 1$ *s.t.* $I + x \in \mathscr{I}$.

Independence Axioms

Independent Sets	*Independent Spaces*
(i1) $\emptyset \in \mathscr{I}$.	*(I1)* $0 \in \mathscr{I}$.
(i2) If $I \subseteq J, J \in \mathscr{I} \implies I \in \mathscr{I}$.	*(I2) If* $I \leq J, J \in \mathscr{I} \implies I \in \mathscr{I}$.
(i3) If $I, J \in \mathscr{I}$, $\lvert I \rvert < \lvert J \rvert$ *then* $\exists\, x \in J \backslash I$ *s.t.* $\{x\} \cup I \in \mathscr{I}$.	*(I3) If* $I, J \in \mathscr{I}$, $\dim(I) < \dim(J)$ *then* $\exists\, x \leq J, x \nleq I$, $\dim(x) = 1$ *s.t.* $I + x \in \mathscr{I}$.
	(I4) If $I \leq A$, $J \leq B$, $I, J \in \mathscr{I}$, *max'l in* A, B *then* $A + B$ *has a max'l ind. subspace in* $I + J$.

Independence Axioms

Independent Sets	*Independent Spaces*
(i1) $\emptyset \in \mathscr{I}$. *(i2) If* $I \subseteq J, J \in \mathscr{I} \implies I \in \mathscr{I}$. *(i3) If* $I, J \in \mathscr{I}$, $\lvert I\rvert < \lvert J\rvert$ *then* $\exists\, x \in J \backslash I$ *s.t.* $\{x\} \cup I \in \mathscr{I}$.	*(I1)* $0 \in \mathscr{I}$. *(I2) If* $I \leq J, J \in \mathscr{I} \implies I \in \mathscr{I}$. *(I3) If* $I, J \in \mathscr{I}$, $\dim(I) < \dim(J)$ *then* $\exists\, x \leq J, x \not\leq I$, $\dim(x) = 1$ *s.t.* $I + x \in \mathscr{I}$.
	(I4) If $I \leq A$, $J \leq B$, $I, J \in \mathscr{I}$, *max'l in* A, B *then* $A + B$ *has a max'l ind. subspace in* $I + J$.

Define

$$r(A) := \max\{\dim(I) : I \leq A, I \in \mathscr{I}\} \text{ for all } A \leq E.$$

Independence Axioms

Independent Sets	*Independent Spaces*
(i1) $\emptyset \in \mathscr{I}$.	*(I1)* $0 \in \mathscr{I}$.
(i2) If $I \subseteq J, J \in \mathscr{I} \implies I \in \mathscr{I}$.	*(I2) If* $I \leq J, J \in \mathscr{I} \implies I \in \mathscr{I}$.
(i3) If $I, J \in \mathscr{I}$, $\|I\| < \|J\|$ *then* $\exists\, x \in J \backslash I$ *s.t.* $\{x\} \cup I \in \mathscr{I}$.	*(I3) If* $I, J \in \mathscr{I}$, $\dim(I) < \dim(J)$ *then* $\exists\, x \leq J, x \not\leq I$, $\dim(x) = 1$ *s.t.* $I + x \in \mathscr{I}$.
	(I4) If $I \leq A$, $J \leq B$, $I, J \in \mathscr{I}$, *max'l in* A, B *then* $A + B$ *has a max'l ind. subspace in* $I + J$.

Define

$$r(A) := \max\{\dim(I) : I \leq A, I \in \mathscr{I}\} \text{ for all } A \leq E.$$

If (I1)-(I3) hold but (I4) does not, we can cook up examples violating submodularity.

Independence Axioms

Independent Sets	*Independent Spaces*
(i1) $\emptyset \in \mathscr{I}$. *(i2) If* $I \subseteq J, J \in \mathscr{I} \implies I \in \mathscr{I}$. *(i3) If* $I, J \in \mathscr{I}$, $\lvert I\rvert < \lvert J\rvert$ *then* $\exists\, x \in J \backslash I$ *s.t.* $\{x\} \cup I \in \mathscr{I}$.	*(I1)* $0 \in \mathscr{I}$. *(I2) If* $I \leq J, J \in \mathscr{I} \implies I \in \mathscr{I}$. *(I3) If* $I, J \in \mathscr{I}$, $\dim(I) < \dim(J)$ *then* $\exists\, x \leq J, x \not\leq I$, $\dim(x) = 1$ *s.t.* $I + x \in \mathscr{I}$.
	(I4) If $I \leq A$, $J \leq B$, $I, J \in \mathscr{I}$, *max'l in* A, B *then* $A + B$ *has a max'l ind. subspace in* $I + J$.

Define

$$r(A) := \max\{\dim(I) : I \leq A, I \in \mathscr{I}\} \text{ for all } A \leq E.$$

If (I1)-(I3) hold but (I4) does not, we can cook up examples violating submodularity.

Example

Let $\mathscr{I} := \{0, \langle 1100\rangle, \langle 0011\rangle, \langle 1111\rangle, \langle 1100, 0011\rangle\} \subset \mathbb{F}_2^4$. $\mathscr{I}$ satisfies (I1)-(I3), fails (I4).

Let $A = \langle 1100, 0001\rangle$, $B = \langle 1100, 0010\rangle$. So $A + B = \langle 1100, 0011, 0010\rangle$, $A \cap B = \langle 1100\rangle$.

$$r(A+B) + r(A \cap B) = 2 + 1 \not\leq r(A) + r(B) = 1 + 1.$$

Independence Axioms

Independent Sets	*Independent Spaces*
(i1) $\emptyset \in \mathscr{I}$.	*(I1)* $0 \in \mathscr{I}$.
(i2) If $I \subseteq J, J \in \mathscr{I} \implies I \in \mathscr{I}$.	*(I2) If* $I \leq J, J \in \mathscr{I} \implies I \in \mathscr{I}$.
(i3) If $I, J \in \mathscr{I}$, $\lvert I\rvert < \lvert J\rvert$ *then*	*(I3) If* $I, J \in \mathscr{I}$, $\dim(I) < \dim(J)$ *then*
$\exists\, x \in J \backslash I$ *s.t.* $\{x\} \cup I \in \mathscr{I}$.	$\exists\, x \leq J, x \nleq I$, $\dim(x) = 1$ *s.t.* $I + x \in \mathscr{I}$.
	(I4) If $I \leq A$, $I \in \mathscr{I}$, *max'l in* A, $\dim(x) = 1$
	then $A + x$ *has a max'l ind. subspace in* $I + x$.

Define

$$r(A) := \max\{\dim(I) : I \leq A, I \in \mathscr{I}\} \text{ for all } A \leq E.$$

If (I1)-(I3) hold but (I4) does not, we can cook up examples violating submodularity.

Example

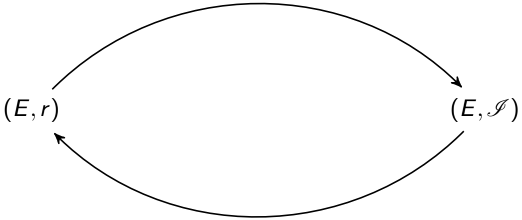
Let $\mathscr{I} := \{0, \langle 1100\rangle, \langle 0011\rangle, \langle 1111\rangle, \langle 1100, 0011\rangle\} \subset \mathbb{F}_2^4$. $\mathscr{I}$ satisfies (I1)-(I3), fails (I4).

Let $A = \langle 1100, 0001\rangle$, $B = \langle 1100, 0010\rangle$. So $A + B = \langle 1100, 0011, 0010\rangle$, $A \cap B = \langle 1100\rangle$.

$$r(A+B) + r(A \cap B) = 3 \nleq 2 = r(A) + r(B).$$

Theorem (Jurrius, Pellikaan 2018)

1. *Let $\mathscr{I}$ be a family of subspaces of E that satisfies the flat axioms (I1)-(I4).*
   Then $(E, \mathscr{I})$ determines a q-matroid $(E, r_{\mathscr{I}})$ whose set of independent spaces is $\mathscr{I}$.
2. *Let (E, r) be a q-matroid with independent spaces $\mathscr{I}_r$.*
   Then $\mathscr{I}_r$ satisfies axioms (I1)-(I4).
3. $r_{\mathscr{I}_r} = r$ *and* $\mathscr{I} r_{\mathscr{I}}$.



Independent Spaces in a Representable q-Matroid

Let $G \in \mathbb{F}_{q^m}^{k \times n}$ have rank k. Let $Y \in \mathbb{F}_q^{r \times n}$. If $R_Y := \mathrm{row}_{\mathbb{F}_q}(Y)$ then $r(R_Y) = \mathrm{rk}_{\mathbb{F}_{q^m}}(GY^T)$.

Let $G \in \mathbb{F}_{q^m}^{k\times n}$ have rank k. Let $Y \in \mathbb{F}_q^{r\times n}$. If $R_Y := \mathrm{row}_{\mathbb{F}_q}(Y)$ then $r(R_Y) = \mathrm{rk}_{\mathbb{F}_{q^m}}(GY^T)$.

$M[G] := (\mathbb{F}_q^n, r)$ is the representable q-matroid determined by (the rowspace of) G.

Let $G \in \mathbb{F}_{q^m}^{k\times n}$ have rank k. Let $Y \in \mathbb{F}_q^{r\times n}$. If $R_Y := \mathrm{row}_{\mathbb{F}_q}(Y)$ then $r(R_Y) = \mathrm{rk}_{\mathbb{F}_{q^m}}(GY^T)$.

$M[G] := (\mathbb{F}_q^n, r)$ is the representable q-matroid determined by (the rowspace of) G.

G is the generator matrix of an $\mathbb{F}_{q^m}$-$[n,k]$ code C and is the PCM of an $\mathbb{F}_{q^m}$-$[n,n-k]$ code $C^\perp$.

$$C^\perp = \{y \in \mathbb{F}_{q^m}^n : Gy^T = 0\}.$$

Independent Spaces in a Representable q-Matroid

Let $G \in \mathbb{F}_{q^m}^{k\times n}$ have rank k. Let $Y \in \mathbb{F}_q^{r\times n}$. If $R_Y := \mathrm{row}_{\mathbb{F}_q}(Y)$ then $r(R_Y) = \mathrm{rk}_{\mathbb{F}_{q^m}}(GY^T)$.

$M[G] := (\mathbb{F}_q^n, r)$ is the representable q-matroid determined by (the rowspace of) G.

G is the generator matrix of an $\mathbb{F}_{q^m}$-$[n,k]$ code C and is the PCM of an $\mathbb{F}_{q^m}$-$[n,n-k]$ code $C^\perp$.

$$C^\perp = \{y \in \mathbb{F}_{q^m}^n : Gy^T = 0\}.$$

Let $y \in \mathbb{F}_{q^m}^n$ s.t. $\mathrm{rk}(y) := \mathrm{rk}_{\mathbb{F}_q}(\langle y_1,\dots,y_n\rangle) = r$. Then $y = zY$ some $z \in \mathbb{F}_{q^m}^r$, $\mathrm{rk}(z) = r$.

We say that y has **support** equal to R_Y.

Let $G \in \mathbb{F}_{q^m}^{k\times n}$ have rank k. Let $Y \in \mathbb{F}_q^{r\times n}$. If $R_Y := \mathrm{row}_{\mathbb{F}_q}(Y)$ then $r(R_Y) = \mathrm{rk}_{\mathbb{F}_{q^m}}(GY^T)$.

$M[G] := (\mathbb{F}_q^n, r)$ is the representable q-matroid determined by (the rowspace of) G.

G is the generator matrix of an $\mathbb{F}_{q^m}$-$[n,k]$ code C and is the PCM of an $\mathbb{F}_{q^m}$-$[n,n-k]$ code $C^\perp$.

$$C^\perp = \{y \in \mathbb{F}_{q^m}^n : Gy^T = 0\}.$$

Let $y \in \mathbb{F}_{q^m}^n$ s.t. $\mathrm{rk}(y) := \mathrm{rk}_{\mathbb{F}_q}(\langle y_1, \ldots, y_n\rangle) = r$. Then $y = zY$ some $z \in \mathbb{F}_{q^m}^r$, $\mathrm{rk}(z) = r$.

We say that y has **support** equal to R_Y.

So $Gy^T = 0 \Leftrightarrow GY^Tz^T = 0 \implies \mathrm{rk}_{\mathbb{F}_{q^m}}(GY^T) < r$.
Conversely, $\mathrm{rk}_{\mathbb{F}_{q^m}}(GY^T) < r \implies GY^Tv^T = 0$ some $v, \Leftrightarrow Gz^T = 0, z = vY$.

Independent Spaces in a Representable q-Matroid

Let $G \in \mathbb{F}_{q^m}^{k\times n}$ have rank k. Let $Y \in \mathbb{F}_q^{r\times n}$. If $R_Y := \mathrm{row}_{\mathbb{F}_q}(Y)$ then $r(R_Y) = \mathrm{rk}_{\mathbb{F}_{q^m}}(GY^T)$.

$M[G] := (\mathbb{F}_q^n, r)$ is the representable q-matroid determined by (the rowspace of) G.

G is the generator matrix of an $\mathbb{F}_{q^m}$-$[n,k]$ code C and is the PCM of an $\mathbb{F}_{q^m}$-$[n,n-k]$ code $C^\perp$.

$$C^\perp = \{y \in \mathbb{F}_{q^m}^n : Gy^T = 0\}.$$

Let $y \in \mathbb{F}_{q^m}^n$ s.t. $\mathrm{rk}(y) := \mathrm{rk}_{\mathbb{F}_q}(\langle y_1, \ldots, y_n\rangle) = r$. Then $y = zY$ some $z \in \mathbb{F}_{q^m}^r$, $\mathrm{rk}(z) = r$.

We say that y has **support** equal to R_Y.

So $Gy^T = 0 \Leftrightarrow GY^Tz^T = 0 \implies \mathrm{rk}_{\mathbb{F}_{q^m}}(GY^T) < r$.
Conversely, $\mathrm{rk}_{\mathbb{F}_{q^m}}(GY^T) < r \implies GY^Tv^T = 0$ some $v, \Leftrightarrow Gz^T = 0, z = vY$.

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

A space is independent in $M[G]$ iff it is not the support of an element of $C^\perp$.

Closure Axioms

$\mathrm{cl}: 2^E \longrightarrow 2^E$	$\mathrm{Cl}: \mathscr{L}(E) \longrightarrow \mathscr{L}(E)$
(cl1) $A \subseteq \mathrm{cl}(A)$.	*(Cl1)* $A \leq \mathrm{cl}(A)$.
(cl2) $A \subseteq B \implies \mathrm{cl}(A) \subseteq \mathrm{cl}(B)$.	*(Cl2)* $A \leq B \implies \mathrm{cl}(A) \leq \mathrm{cl}(B)$.
(cl3) $\mathrm{cl}(A) = \mathrm{cl}(\mathrm{cl}(A))$.	*(Cl3)* $\mathrm{cl}(A) = \mathrm{cl}(\mathrm{cl}(A))$.
(cl4) If $y \subseteq \mathrm{cl}(A+x)$ *and* $y \not\subseteq \mathrm{cl}(A)$ *then* $x \subseteq \mathrm{cl}(A+y)$.	*(Cl4) If* $y \leq \mathrm{cl}(A+x)$ *and* $y \not\leq \mathrm{cl}(A)$ *then* $x \leq \mathrm{cl}(A+y)$.

Closure Axioms

$\mathrm{cl}: 2^E \longrightarrow 2^E$	$\mathrm{Cl}: \mathscr{L}(E) \longrightarrow \mathscr{L}(E)$
(cl1) $A \subseteq \mathrm{cl}(A)$. *(cl2)* $A \subseteq B \implies \mathrm{cl}(A) \subseteq \mathrm{cl}(B)$. *(cl3)* $\mathrm{cl}(A) = \mathrm{cl}(\mathrm{cl}(A))$. *(cl4) If* $y \subseteq \mathrm{cl}(A+x)$ *and* $y \not\subseteq \mathrm{cl}(A)$ *then* $x \subseteq \mathrm{cl}(A+y)$.	*(Cl1)* $A \leq \mathrm{cl}(A)$. *(Cl2)* $A \leq B \implies \mathrm{cl}(A) \leq \mathrm{cl}(B)$. *(Cl3)* $\mathrm{cl}(A) = \mathrm{cl}(\mathrm{cl}(A))$. *(Cl4) If* $y \leq \mathrm{cl}(A+x)$ *and* $y \not\leq \mathrm{cl}(A)$ *then* $x \leq \mathrm{cl}(A+y)$.
$\mathscr{I}_{\mathrm{cl}} := \{X \subseteq E : e \notin \mathrm{cl}(X-e) \text{ any } e \in X\}$	$\mathscr{I}_{\mathrm{Cl}} := \{X \leq E : \mathrm{Cl}(X) \neq \mathrm{Cl}(A), A < X\}$

Closure Axioms

$\mathrm{cl}: 2^E \longrightarrow 2^E$	$\mathrm{Cl}: \mathscr{L}(E) \longrightarrow \mathscr{L}(E)$
(cl1) $A \subseteq \mathrm{cl}(A)$. *(cl2)* $A \subseteq B \implies \mathrm{cl}(A) \subseteq \mathrm{cl}(B)$. *(cl3)* $\mathrm{cl}(A) = \mathrm{cl}(\mathrm{cl}(A))$. *(cl4)* *If* $y \subseteq \mathrm{cl}(A+x)$ *and* $y \not\subseteq \mathrm{cl}(A)$ *then* $x \subseteq \mathrm{cl}(A+y)$.	*(Cl1)* $A \leq \mathrm{cl}(A)$. *(Cl2)* $A \leq B \implies \mathrm{cl}(A) \leq \mathrm{cl}(B)$. *(Cl3)* $\mathrm{cl}(A) = \mathrm{cl}(\mathrm{cl}(A))$. *(Cl4)* *If* $y \leq \mathrm{cl}(A+x)$ *and* $y \not\leq \mathrm{cl}(A)$ *then* $x \leq \mathrm{cl}(A+y)$.
$\mathscr{I}_{\mathrm{cl}} := \{X \subseteq E : e \notin \mathrm{cl}(X-e)$ *any* $e \in X\}$	$\mathscr{I}_{\mathrm{Cl}} := \{X \leq E : \mathrm{Cl}(X) \neq \mathrm{Cl}(A), A < X\}$

Example

Let $1 \leq k \leq n$. Define a map

$$\mathrm{Cl}: \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n : A \mapsto \begin{cases} A & \text{if } \dim(A) \leq k-1 \\ E & \text{otherwise} \end{cases}$$

Closure Axioms

$\mathrm{cl}: 2^E \longrightarrow 2^E$	$\mathrm{Cl}: \mathscr{L}(E) \longrightarrow \mathscr{L}(E)$
(cl1) $A \subseteq \mathrm{cl}(A)$. *(cl2)* $A \subseteq B \implies \mathrm{cl}(A) \subseteq \mathrm{cl}(B)$. *(cl3)* $\mathrm{cl}(A) = \mathrm{cl}(\mathrm{cl}(A))$. *(cl4) If* $y \subseteq \mathrm{cl}(A+x)$ *and* $y \not\subseteq \mathrm{cl}(A)$ *then* $x \subseteq \mathrm{cl}(A+y)$.	*(Cl1)* $A \leq \mathrm{cl}(A)$. *(Cl2)* $A \leq B \implies \mathrm{cl}(A) \leq \mathrm{cl}(B)$. *(Cl3)* $\mathrm{cl}(A) = \mathrm{cl}(\mathrm{cl}(A))$. *(Cl4) If* $y \leq \mathrm{cl}(A+x)$ *and* $y \not\leq \mathrm{cl}(A)$ *then* $x \leq \mathrm{cl}(A+y)$.
$\mathscr{I}_{\mathrm{cl}} := \{X \subseteq E : e \notin \mathrm{cl}(X-e) \text{ any } e \in X\}$	$\mathscr{I}_{\mathrm{Cl}} := \{X \leq E : \mathrm{Cl}(X) \neq \mathrm{Cl}(A), A < X\}$

Example

Let $1 \leq k \leq n$. Define a map

$$\mathrm{Cl}: \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n : A \mapsto \begin{cases} A & \text{if } \dim(A) \leq k-1 \\ E & \text{otherwise} \end{cases}$$

If $\dim(I) \leq k-1$ then for $J < I$, $\mathrm{Cl}(J) = J \neq I = \mathrm{Cl}(I)$, so $I \in \mathscr{I}_{\mathrm{Cl}}$.

Closure Axioms

$\mathrm{cl} : 2^E \longrightarrow 2^E$	$\mathrm{Cl} : \mathscr{L}(E) \longrightarrow \mathscr{L}(E)$
(cl1) $A \subseteq \mathrm{cl}(A)$. *(cl2)* $A \subseteq B \implies \mathrm{cl}(A) \subseteq \mathrm{cl}(B)$. *(cl3)* $\mathrm{cl}(A) = \mathrm{cl}(\mathrm{cl}(A))$. *(cl4) If* $y \subseteq \mathrm{cl}(A+x)$ *and* $y \not\subseteq \mathrm{cl}(A)$ *then* $x \subseteq \mathrm{cl}(A+y)$.	*(Cl1)* $A \leq \mathrm{cl}(A)$. *(Cl2)* $A \leq B \implies \mathrm{cl}(A) \leq \mathrm{cl}(B)$. *(Cl3)* $\mathrm{cl}(A) = \mathrm{cl}(\mathrm{cl}(A))$. *(Cl4) If* $y \leq \mathrm{cl}(A+x)$ *and* $y \not\leq \mathrm{cl}(A)$ *then* $x \leq \mathrm{cl}(A+y)$.
$\mathscr{I}_{\mathrm{cl}} := \{X \subseteq E : e \notin \mathrm{cl}(X-e) \text{ any } e \in X\}$	$\mathscr{I}_{\mathrm{Cl}} := \{X \leq E : \mathrm{Cl}(X) \neq \mathrm{Cl}(A), A < X\}$

Example

Let $1 \leq k \leq n$. Define a map

$$\mathrm{Cl} : \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n : A \mapsto \begin{cases} A & \text{if } \dim(A) \leq k-1 \\ E & \text{otherwise} \end{cases}$$

If $\dim(I) \leq k-1$ then for $J < I$, $\mathrm{Cl}(J) = J \neq I = \mathrm{Cl}(I)$, so $I \in \mathscr{I}_{\mathrm{Cl}}$.

If $\dim(I) = k$ then for $J < I$, $\mathrm{Cl}(J) = I \neq E = \mathrm{Cl}(I)$, so $I \in \mathscr{I}_{\mathrm{Cl}}$.

Closure Axioms

$\mathrm{cl}: 2^E \longrightarrow 2^E$	$\mathrm{Cl}: \mathscr{L}(E) \longrightarrow \mathscr{L}(E)$
(cl1) $A \subseteq \mathrm{cl}(A)$. *(cl2)* $A \subseteq B \implies \mathrm{cl}(A) \subseteq \mathrm{cl}(B)$. *(cl3)* $\mathrm{cl}(A) = \mathrm{cl}(\mathrm{cl}(A))$. *(cl4) If* $y \subseteq \mathrm{cl}(A+x)$ *and* $y \not\subseteq \mathrm{cl}(A)$ *then* $x \subseteq \mathrm{cl}(A+y)$.	*(Cl1)* $A \leq \mathrm{cl}(A)$. *(Cl2)* $A \leq B \implies \mathrm{cl}(A) \leq \mathrm{cl}(B)$. *(Cl3)* $\mathrm{cl}(A) = \mathrm{cl}(\mathrm{cl}(A))$. *(Cl4) If* $y \leq \mathrm{cl}(A+x)$ *and* $y \not\leq \mathrm{cl}(A)$ *then* $x \leq \mathrm{cl}(A+y)$.
$\mathscr{I}_{\mathrm{cl}} := \{X \subseteq E : e \notin \mathrm{cl}(X-e) \text{ any } e \in X\}$	$\mathscr{I}_{\mathrm{Cl}} := \{X \leq E : \mathrm{Cl}(X) \neq \mathrm{Cl}(A), A < X\}$

Example

Let $1 \leq k \leq n$. Define a map

$$\mathrm{Cl}: \mathbb{F}_q^n \longrightarrow \mathbb{F}_q^n : A \mapsto \begin{cases} A & \text{if } \dim(A) \leq k-1 \\ E & \text{otherwise} \end{cases}$$

If $\dim(I) \leq k-1$ then for $J < I$, $\mathrm{Cl}(J) = J \neq I = \mathrm{Cl}(I)$, so $I \in \mathscr{I}_{\mathrm{Cl}}$.

If $\dim(I) = k$ then for $J < I$, $\mathrm{Cl}(J) = I \neq E = \mathrm{Cl}(I)$, so $I \in \mathscr{I}_{\mathrm{Cl}}$.

If $\dim(A) > k$ then there exists $B < A$, $\dim(B) = k$, so $\mathrm{Cl}(B) = E = \mathrm{Cl}(A)$ and $A \notin \mathscr{I}_{\mathrm{Cl}}$.

Theorem (B., Ceria, Jurrius, 2021)

1. *Let* $\mathrm{Cl} : \mathscr{L}(E) \longrightarrow \mathscr{L}(E)$ *be a closure function. Then* $(E, \mathscr{I}_{\mathrm{Cl}})$ *satisfies (I1)-(I4).*
2. (E, Cl) *determines a q-matroid* (E, r) *whose set of independent spaces is*

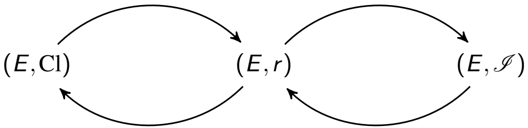
$$\mathscr{I}_{\mathrm{Cl}} := \{X \leq E : \mathrm{Cl}(X) \neq \mathrm{Cl}(A), A < X\}$$

   and whose closure function satisfies $\mathrm{Cl}_r = \mathrm{Cl}$.

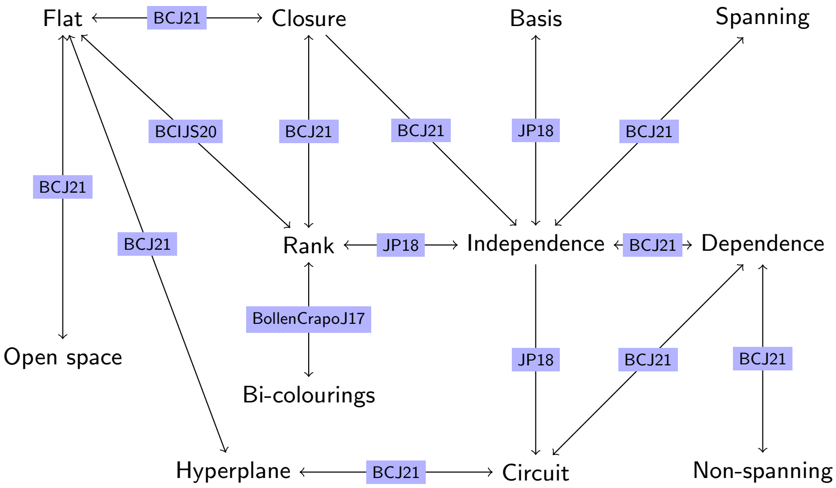
3. *Let* $(E, \mathscr{I})$ *satisfy (I1)-(I4). Define*

$$r_{\mathscr{I}} : \mathscr{L}(E) \longrightarrow \mathbb{Z} : A \mapsto \max\{\dim(I) : I \in \mathscr{I}, I \subseteq A\}.$$

   Then $(E, \mathscr{I})$ *determines a q-matroid* (E, r) *whose closure function is* $\mathrm{Cl}_{\mathscr{I}} = \mathrm{Cl}_r$ *and whose set of independent spaces is* $\mathscr{I}$.



More q-Cryptomorphisms



Circuit Axioms

Circuit (Sets)	*Circuits (Spaces)*
(c1) $\emptyset \notin \mathscr{C}$.	*(C1)* $0 \notin \mathscr{C}$.
(c2) $C_1, C_2 \in \mathscr{C}, C_1 \neq C_2 \implies C_1 \nsubseteq C_2$.	*(C2)* $C_1, C_2 \in \mathscr{C}, C_1 \neq C_2 \implies C_1 \nleq C_2$.
(c3) $C_1, C_2 \in \mathscr{C}, C_1 \neq C_2, x \in C_1 \cap C_2$	*(C3)* $C_1, C_2 \in \mathscr{C}, C_1 \neq C_2, x \leq C_1 \cap C_2$
$\implies \exists C_3 \in \mathscr{C}$ *s.t.* $C_3 \subseteq (C_1 \cup C_2) - \{x\}$.	$\implies \exists C_3 \in \mathscr{C}$ *s.t.* $C_3 \leq C_1 + C_2, x \nleq C_3$.

Circuit Axioms

Circuit (Sets)	*Circuits (Spaces)*
(c1) $\emptyset \notin \mathscr{C}$.	*(C1)* $0 \notin \mathscr{C}$.
(c2) $C_1, C_2 \in \mathscr{C}, C_1 \neq C_2 \implies C_1 \nsubseteq C_2$.	*(C2)* $C_1, C_2 \in \mathscr{C}, C_1 \neq C_2 \implies C_1 \nleq C_2$.
(c3) $C_1, C_2 \in \mathscr{C}, C_1 \neq C_2, x \in C_1 \cap C_2$	*(C3)* $C_1, C_2 \in \mathscr{C}, C_1 \neq C_2, x \leq C_1 \cap C_2$
$\implies \exists C_3 \in \mathscr{C}$ *s.t.* $C_3 \subseteq (C_1 \cup C_2) - \{x\}$.	$\implies \exists C_3 \in \mathscr{C}$ *s.t.* $C_3 \leq C_1 + C_2, x \nleq C_3$.

In fact (C3) is too weak to define a q-matroid.

Circuit Axioms

Circuit (Sets)	*Circuits (Spaces)*
(c1) $\emptyset \notin \mathscr{C}$.	*(C1)* $0 \notin \mathscr{C}$.
(c2) $C_1, C_2 \in \mathscr{C}, C_1 \neq C_2 \implies C_1 \nsubseteq C_2$.	*(C2)* $C_1, C_2 \in \mathscr{C}, C_1 \neq C_2 \implies C_1 \nleq C_2$.
(c3) $C_1, C_2 \in \mathscr{C}, C_1 \neq C_2, x \in C_1 \cap C_2$	*(C3)* $C_1, C_2 \in \mathscr{C}, C_1 \neq C_2, x \leq C_1 \cap C_2$
$\implies \exists C_3 \in \mathscr{C}$ *s.t.* $C_3 \subseteq (C_1 \cup C_2) - \{x\}$.	$\implies \exists C_3 \in \mathscr{C}$ *s.t.* $C_3 \leq C_1 + C_2, x \nleq C_3$.

In fact (C3) is too weak to define a q-matroid.

Example

Let $\mathscr{I} := \{0, \langle 1100 \rangle, \langle 0011 \rangle, \langle 1111 \rangle, \langle 1100, 0011 \rangle\} \subset \mathbb{F}_2^4$.

$\mathscr{C}$ is the collection of minimal dependent spaces.

Therefore, $\mathscr{C}$ is the set of 1-dim'l spaces not in $\mathscr{I}$.

Moreover, $\mathscr{C}$ satisfies (C1)-(C3).

As we saw before, $(E, \mathscr{I})$ does not define a q-matroid (it fails (I4) and (R3)).

Circuit Axioms

Circuit (Sets)	*Circuits (Spaces)*
(c1) $\emptyset \notin \mathscr{C}$.	*(C1)* $0 \notin \mathscr{C}$.
(c2) $C_1, C_2 \in \mathscr{C}, C_1 \neq C_2 \implies C_1 \not\subseteq C_2$.	*(C2)* $C_1, C_2 \in \mathscr{C}, C_1 \neq C_2 \implies C_1 \not\leq C_2$.
(c3) $C_1, C_2 \in \mathscr{C}, C_1 \neq C_2, x \in C_1 \cap C_2$	*(C3)* $C_1, C_2 \in \mathscr{C}, C_1 \neq C_2, X \leq C_1 + C_2 = D$
$\implies \exists C_3 \in \mathscr{C}$ *s.t.* $C_3 \subseteq (C_1 \cup C_2) - \{x\}$.	$\mathrm{codim}_D(X) = 1 \implies \exists C_3 \in \mathscr{C}$ *s.t.* $C_3 \leq X$.

Circuit Axioms

Circuit (Sets)	*Circuits (Spaces)*
(c1) $\emptyset \notin \mathscr{C}$.	*(C1)* $0 \notin \mathscr{C}$.
(c2) $C_1, C_2 \in \mathscr{C}, C_1 \neq C_2 \implies C_1 \nsubseteq C_2$.	*(C2)* $C_1, C_2 \in \mathscr{C}, C_1 \neq C_2 \implies C_1 \nleq C_2$.
(c3) $C_1, C_2 \in \mathscr{C}, C_1 \neq C_2, x \in C_1 \cap C_2$ $\implies \exists C_3 \in \mathscr{C}$ *s.t.* $C_3 \subseteq (C_1 \cup C_2) - \{x\}$.	*(C3)* $C_1, C_2 \in \mathscr{C}, C_1 \neq C_2$, $X \leq C_1 + C_2 = D$ $\mathrm{codim}_D(X) = 1 \implies \exists C_3 \in \mathscr{C}$ *s.t.* $C_3 \leq X$.

The new (C3) implies the old (C3). But the old (C3) doesn't include enough of the codim 1 subspaces of $C_1 + C_2$.

Circuit Axioms

Circuit (Sets)	*Circuits (Spaces)*
(c1) $\emptyset \notin \mathscr{C}$.	*(C1)* $0 \notin \mathscr{C}$.
(c2) $C_1, C_2 \in \mathscr{C}, C_1 \neq C_2 \implies C_1 \nsubseteq C_2$.	*(C2)* $C_1, C_2 \in \mathscr{C}, C_1 \neq C_2 \implies C_1 \nleq C_2$.
(c3) $C_1, C_2 \in \mathscr{C}, C_1 \neq C_2, x \in C_1 \cap C_2$	*(C3)* $C_1, C_2 \in \mathscr{C}, C_1 \neq C_2,\ X \leq C_1 + C_2 = D$
$\implies \exists C_3 \in \mathscr{C}$ *s.t.* $C_3 \subseteq (C_1 \cup C_2) - \{x\}$.	$\operatorname{codim}_D(X) = 1 \implies \exists C_3 \in \mathscr{C}$ *s.t.* $C_3 \leq X$.

The new (C3) implies the old (C3). But the old (C3) doesn't include enough of the codim 1 subspaces of $C_1 + C_2$.

Example

Let $\mathscr{I} := \{0, \langle 1100 \rangle, \langle 0011 \rangle, \langle 1111 \rangle, \langle 1100, 0011 \rangle\} \subset \mathbb{F}_2^4$.

$\mathscr{C}$ is the collection of minimal dependent spaces.

Therefore, $\mathscr{C}$ is the set of 1-dim'l spaces not in $\mathscr{I}$.

Moreover, $\mathscr{C}$ satisfies (C1), (C2) but fails the new (C3).

Let $C_1 = \langle 1000 \rangle, C_2 = \langle 0111 \rangle$. Then $D = \langle 1111 \rangle$ has codim 1 in $C_1 + C_2$, but $D \in \mathscr{I}$, so the new (C3) fails.

Duality

Matroid	*q-Matroid*
Complement $r^*(A) := \|A\| - r(E) + r(E - A)$	*Orthogonal Complement* $r^*(A) := \dim(A) - r(E) + r(A^\perp)$

Duality

Matroid	*q-Matroid*
Complement	*Orthogonal Complement*
$r^*(A) := \|A\| - r(E) + r(E - A)$	$r^*(A) := \dim(A) - r(E) + r(A^\perp)$

- $A^\perp := \{x \in E : \langle x, a \rangle = 0 \, \forall a \in A\}$, $\langle \cdot, \cdot \rangle$ is a bilinear form on E.
- $A \in \mathscr{I}^* \Leftrightarrow r(A^\perp) = r(E)$.
- $M^{**} = M$.

Duality

Matroid	*q-Matroid*
Complement	*Orthogonal Complement*
$r^*(A) := \|A\| - r(E) + r(E - A)$	$r^*(A) := \dim(A) - r(E) + r(A^\perp)$

- $A^\perp := \{x \in E : \langle x, a \rangle = 0 \, \forall a \in A\}$, $\langle \cdot, \cdot \rangle$ is a bilinear form on E.
- $A \in \mathscr{I}^* \Leftrightarrow r(A^\perp) = r(E)$.
- $M^{**} = M$.

Example (Jurrius, Pellikaan, 2018)

If $M = M[G]$ for a $k \times n$ matrix G of rank k over $\mathbb{F}_{q^m}$ then $M^* = M[H]$ for an $(n-k) \times n$ matrix H of rank $n-k$ over $\mathbb{F}_{q^m}$ s.t. $GH^T = 0$.

The dependent spaces of M are the supports of elements in $\mathrm{nullspace}(G) = \mathrm{row}(H)$.

$r^*(R_Y) = \mathrm{rk}(Y) - k + r(R_Y^\perp) = \mathrm{rk}(Y) - k + \mathrm{rk}(GX^T) = \mathrm{rk}(HY^T)$.

Contraction and Restriction

Matroid	*q-Matroid*
Restriction to $X \subseteq E$ $M\|X := (X, r)$	*Restriction to* $X \leq E$ $M\|X := (X, r)$
Deletion of $X \subseteq E$ $M \backslash X := M\|(E - X)$	*Deletion of* $X \leq E$ $M \backslash X := M\|X^{\perp}$
Contraction of $X \subseteq E$ $M/X := (E - X, r_{M/X})$ $r_{M/X}(A) = r(A \cup X) - r(X)$	*Contraction of* $X \leq E$ $M/X := (E/X, r_{M/X})$ $r_{M/X}(A/X) = r(A) - r(X)$
$(M/T) := (M^{*}\mathrm{T})^{*}$	$(M/T)^{*} \cong M^{*}\|_{T^{\perp}}$

$(M/T)^{*} \cong M^{*}|_{T^{\perp}}$ are **lattice-equivalent**.

The choice of bilinear forms used in duality gives different but equivalent matroids.

q-Matroids Induced by q-Steiner Systems - Defining a Matroid by Flats

Theorem (B., Ceria, Ionica, Jurrius, Saçıkara, 2020)

Let $\mathscr{S}$ be a q-Steiner system with blocks $\mathscr{B}$. Define the family

$$\mathscr{F} = \left\{ \bigcap_{B \in S} B : S \subseteq \mathscr{B} \right\}.$$

1. *$\mathscr{F}$ is the collection of flats of a q-perfect matroid design (E, r).*

q-Matroids Induced by q-Steiner Systems - Defining a Matroid by Flats

Theorem (B., Ceria, Ionica, Jurrius, Saçıkara, 2020)

Let $\mathscr{S}$ be a q-Steiner system with blocks $\mathscr{B}$. Define the family

$$\mathscr{F} = \left\{ \bigcap_{B \in S} B : S \subseteq \mathscr{B} \right\}.$$

1. *$\mathscr{F}$ is the collection of flats of a q-perfect matroid design (E, r).*
2. $r(A) = \begin{cases} \dim(A) & \text{if } \dim(A) \leq t, \\ t & \text{if } \dim(A) > t \text{ and } A \text{ is contained in a block of } \mathscr{B}, \\ t+1 & \text{if } \dim(A) > t \text{ and } A \text{ is not contained in a block of } \mathscr{B}. \end{cases}$

Theorem (B., Ceria, Ionica, Jurrius, Saçıkara, 2020)

Let $\mathscr{S}$ be a q-Steiner system with blocks $\mathscr{B}$. Define the family

$$\mathscr{F} = \left\{ \bigcap_{B \in S} B : S \subseteq \mathscr{B} \right\}.$$

1. *$\mathscr{F}$ is the collection of flats of a q-perfect matroid design (E, r).*
2. $r(A) = \begin{cases} \dim(A) & \text{if } \dim(A) \leq t, \\ t & \text{if } \dim(A) > t \text{ and } A \text{ is contained in a block of } \mathscr{B}, \\ t+1 & \text{if } \dim(A) > t \text{ and } A \text{ is not contained in a block of } \mathscr{B}. \end{cases}$
3. *$I \leq E$ is independent if*
   - $\dim(I) \leq t$ *or*
   - $\dim(I) = t+1$ *and I is not in a block of $\mathscr{B}$.*

Theorem (B., Ceria, Ionica, Jurrius, Saçıkara, 2020)

Let $\mathscr{S}$ be a q-Steiner system with blocks $\mathscr{B}$. Define the family

$$\mathscr{F} = \left\{ \bigcap_{B \in S} B : S \subseteq \mathscr{B} \right\}.$$

1. *$\mathscr{F}$ is the collection of flats of a q-perfect matroid design (E, r).*
2. $$r(A) = \begin{cases} \dim(A) & \text{if } \dim(A) \leq t, \\ t & \text{if } \dim(A) > t \text{ and } A \text{ is contained in a block of } \mathscr{B}, \\ t+1 & \text{if } \dim(A) > t \text{ and } A \text{ is not contained in a block of } \mathscr{B}. \end{cases}$$
3. *$I \leq E$ is independent if*
   - $\dim(I) \leq t$ *or*
   - $\dim(I) = t+1$ *and I is not in a block of $\mathscr{B}$.*
4. *$C \leq E$ is a circuit if*
   - $\dim C = t+1$ *and C is contained in a block of $\mathscr{B}$ or*
   - $\dim C = t+2$ *and all $(t+1)$-subspaces of C are contained in none of the blocks of $\mathscr{B}$.*

Thank you!

Thank you!

- Byrne, Ceria, Jurrius, 'Constructions of New Cryptomorphisms,' 2021 (arXiv:2104.01486).
- Byrne, Ceria, Ionica, Jurrius, 'Weighted Subspace Designs from q-Polymatroids,' 2021 (arXiv:2104.12463).
- Jurrius, Pellikaan, 'Defining the q-analogue of a matroid,' Electronic Journal of Combinatorics, 25(3), 2018.