Three paths to the rank metric

q-(poly)matroids

M. Ceria
Politecnico di Bari

Matroids

$M = (E, r)$, E finite set,

$$r : 2^E \to \mathbb{N}$$
$$A \mapsto r(A)$$

Rank axioms

$\forall A, B \subseteq E$:

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

R2) $A \subseteq B \Rightarrow r(A) \leq r(B)$;

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

Independent sets: cryptomorphism

$M = (E, \mathcal{I})$, E finite set and $\mathcal{I}$ a collection of subsets

I1) $\mathcal{I} \neq \emptyset$;

I2) $J \in \mathcal{I}, I \subseteq J \Rightarrow I \in \mathcal{I}$;

I3) $I, J \in \mathcal{I}, |I| \leq |J| \Rightarrow \exists x \in J \setminus I : I \cup \{x\} \in \mathcal{I}$.

Generalization of the notion of linear independence.

Other cryptomorphisms

Bases

Maximal independent sets.

Circuits

Dependent sets such that all proper subsets are independent.

Representability

$E = \{\text{columns of some matrix M}\}$

$\mathcal{I} = \{B \subseteq E : \; B \text{ cols. L.I.}\}$

$M = (E, \mathcal{I})$ is a matroid and it is called **representable** (over some field).

Vámos

There is no representation whatever field you decide to choose

Duality

$M = (E, r)$ $M^* = (E, r^*)$

$\forall A \subseteq E$

$$r^*(A) = r(E \setminus A) + |A| - r(E)$$

Matroids and codes

C code with generator matrix G.

$$M_G = (E, \mathcal{I}_G)$$

E: columns $\mathcal{I}_G$: linearly independent columns

MDS code $[n, k] \to U_{k,n}$.

$C^\perp$ corresponds to M_G^*.

$P = (S, \rho)$

$S \neq \emptyset$ a finite set

$$\rho : 2^S \to \mathbb{R}^+$$

For each $A, B \subseteq S$:

$\rho_1)$ $\rho(\emptyset) = 0$;

$\rho_2)$ $A \subseteq B \Rightarrow \rho(A) \leq \rho(B)$;

$\rho_3)$ $\rho(A \cup B) + \rho(A \cap B) \leq \rho(A) + \rho(B)$.

Textbooks

Jurrius, Relinde, and Ruud Pellikaan. "Defining the *q*-Analogue of a Matroid." The Electronic Journal of Combinatorics 25.3 (2018): 3-2.

Gorla, E., Jurrius, R., López, H. H., Ravagnani, A. (2020). Rank-metric codes and q-polymatroids. Journal of Algebraic Combinatorics, 52, 1-19.

Passing to the q-analogue

Generalization of combinatorial objects:

finite set $\rightarrow$ **fin. dim. vector space** (over $\mathbb{F}_q$).

To come back: $q \rightarrow 1$.

Passing to the q-analogue

finite set $\rightarrow$ **fin. dim. vector space** (over $\mathbb{F}_q$).

Elements $\rightarrow$ 1-dim. spaces.

Size $\rightarrow$ Dimension

$$n \rightarrow \begin{bmatrix} n \\ 1 \end{bmatrix}_q$$

Union $\rightarrow$ Sum

...

Subspace lattice

n: fixed positive integer; E a fixed n-dimensional vector space over a field, think of $\mathbb{F}_q$.
$\mathcal{L}(E)$: **lattice of subspaces** of E.

Meet: intersection
Join: sum.

q-MATROIDS

$M = (E, r)$
E finite dimensional vector space over ($\mathbb{F}_q$)

RANK FUNCTION

$$r : \{ \text{ subsp. of } E\} \to \mathbb{N}$$

RANK AXIOMS

$\forall A, B \leq E$:

R1) $0 \leq r(A) \leq \dim(A)$;

R2) $A \leq B \Rightarrow r(A) \leq r(B)$;

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

Cryptomorphisms: independent spaces

Not a straightforward q-analogue.

$M = (E, \mathcal{I})$
E finite dimensional vector space over ($\mathbb{F}_q$) $\mathcal{I}$ collection of subspaces of E

Independent axioms

- I1) $\mathcal{I} \neq \emptyset$
- I2) $J \in \mathcal{I}$, $I \leq J$, then $I \in \mathcal{I}$;
- I3) $I, J \in \mathcal{I}$, $\dim(I) < \dim(J)$, then there exists $x \leq J$, $\dim(x) = 1$, $x \nleq I$ such that $I + x \in \mathcal{I}$
- I4) $A, B \leq E$, I, J maximal independent spaces of A and B, respectively, then there is $K \leq I + J$ maximal independent space of $A + B$.

Why 4 axioms?

Other cryptomorphisms

Bases

Maximal independent subspaces.

Circuits

Dependent subspaces such that all proper subsets are independent.

Representability

Let $M = (E, r)$ be a q-matroid of rank k over a field K.
Let $A \subseteq E$ and let Y be a matrix with column space A.

We say that M is **representable** if there exists a $k \times n$ matrix G over an extension field L/K such that $r(A)$ is equal to the matrix rank of GY over L.

Are all q-matroids representable?

Dual q-matroid

Jurrius-Pellikaan

$M = (E, r)$ q-matroid.
$M^* = (E, r^*)$

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

EQUIVALENCE

$M_1 = (E_1, r_1)$, $M_2 = (E_2, r_2)$ q-matroids

LATTICE EQUIVALENT – ISOMORPHIC

there is a lattice isomorphism (bijection, preserves the ordering, the meet and the join)

$$\phi : \mathcal{L}(E_1) \to \mathcal{L}(E_2)$$

such that $r_1(A) = r_2(\phi(A))$, for each $A \leq \mathcal{L}(E_1)$.

q-Polymatroids

GJLR
$P = (E, \rho)$

$E = (\mathbb{F}_q)^n$

$$\rho : \{\text{subspaces of } E\} \to \mathbb{R}^+$$

For each $A, B \leq E$:

ρ_1) $0 \leq \rho(A) \leq \dim(A)$;
ρ_2) $A \subseteq B \Rightarrow \rho(A) \leq \rho(B)$;
ρ_3) $\rho(A+B) + \rho(A \cap B) \leq \rho(A) + \rho(B)$.

If the function ρ takes integer values we have a q–matroid.
Not all q-polymatroids are also q-matroids.

Shiromoto's (q, r)–polymatroid

$P = (E, \rho)$, $E = (\mathbb{F}_q)^n$

$$\rho : \{ \text{ subspace of } E\} \to \mathbb{Z}$$

such that:

For each $A, B \leq E$:

$\rho_1)$ $0 \leq \rho(A) \leq r \dim(A)$;

$\rho_2)$ $A \subseteq B \Rightarrow \rho(A) \leq \rho(B)$;

$\rho_3)$ $\rho(A + B) + \rho(A \cap B) \leq \rho(A) + \rho(B)$.

For $r = 1$ we have a q-matroid.

Shiromoto's (q, r)–polymatroid

The Shiromoto's (q, r)–polymatroid (R, ρ) corresponds to a $(E, \rho/r)$ with the given definition.

If we take a q–polymatroid , which takes values in $\mathbb{Q}$ instead of $\mathbb{R}$, then we get back a (q, r)–polymatroid multiplying the rank by a suitable value r, which eliminates denominators.

GJLR

$((\mathbb{F}_q)^n, \rho_1) \sim ((\mathbb{F}_q)^n, \rho_2)$ if there is a $\mathbb{F}_q$-linear isomorphism

$$\begin{aligned} \phi : & (\mathbb{F}_q)^n \to (\mathbb{F}_q)^n \\ & A \mapsto \phi(A) \end{aligned}$$

such that

$$\forall A \leq (\mathbb{F}_q)^n : \ \rho_1(A) = \rho_2(\phi(A)).$$

Dual q-polymatroid

GJLR

$P = ((\mathbb{F}_q)^n, \rho)$ q-polymatroid. We define the **dual** of P as
$P^* = ((\mathbb{F}_q)^n, \rho^*)$

$\forall A \leq (\mathbb{F}_q)^n$

$$\rho^*(A) = \dim(A) - \rho(P) + \rho(A^\perp),$$

$A^\perp$ orthogonal complement w.r.t. the standard inner product.

Properties of dual q-polymatroids

GJLR - JP

$P = ((\mathbb{F}_q)^n, \rho)$ q-polymatroid.

Then $P^* = ((\mathbb{F}_q)^n, \rho^*)$ is a q-polymatroid as well.

GJLR

$P_1 = ((\mathbb{F}_q)^n, \rho_1), P_2((\mathbb{F}_q)^n, \rho_2)$ two q-polymatroids.

$$P_1 \sim P_2 \Rightarrow P_1^* \sim P_2^*$$

GJLR

$P = ((\mathbb{F}_q)^n, \rho)$ q-polymatroid:

$$P^{**} = P.$$

VRMC AND q-MATROIDS (JP)

$K \subseteq L$ Galois extension

C L-linear VRMC; $J \leq K^n$ K-linear:

$$C(J) = \{\overline{\mathbf{c}} \in C : supp(\overline{\mathbf{c}}) \leq J^{\perp}\}$$

$C(J)$ can be proven to be a L-linear subspace of C.

VRMC and q-matroids (JP)

C VRMC of length n over L; $J \leq K^n$ K-linear; $\dim_K(J) = t$ with generator matrix Y

$$\begin{aligned} \pi_J : & L^n \to L^t \\ & \bar{\mathbf{x}} \mapsto \bar{\mathbf{x}} Y_T \end{aligned}$$

$$C_J := \pi_J(C)$$

VRMC and q-matroids (JP)

$$l(J) := \dim_L(C(J)) \quad r(J) := \dim_L(C_J)$$

Let $\dim_L(C) = k$:

$$l(J) + r(J) = k$$

$E = K^n$, r the rank function given by $r(J) = \dim_L(C_J)$: $M_C = (E, r)$ is a q-matroid.

WARNING

We will consider from now on the matrices in $M_{n,m}(\mathbb{F}_q)$

and we will consider $n, m \geq 2$, $n \leq m$, which is not a problem (otherwise we transpose!)

Notation

For $J \leq (\mathbb{F}_q)^n$:

$$M(J, c) := \{M \in M_{n,m}(\mathbb{F}_q) : colsp(M) \leq J\}$$

For $K \leq (\mathbb{F}_q)^m$:

$$M(K, r) := \{M \in M_{n,m}(\mathbb{F}_q) : rowsp(M) \leq K\}$$

Notation

Let $\mathcal{C} \leq M_{n,m}(\mathbb{F}_q)$ MRMC; we define two subcodes.

For $J \leq (\mathbb{F}_q)^n$:

$$\mathcal{C}(J, c) := \{M \in \mathcal{C} : colsp(M) \leq J\}$$

For $K \leq (\mathbb{F}_q)^m$:

$$\mathcal{C}(K, r) := \{M \in \mathcal{C} : rowsp(M) \leq K\}$$

Notation

Let $\mathcal{C} \leq M_{n,m}(\mathbb{F}_q)$ MRMC; we define two subcodes.

For $J \leq (\mathbb{F}_q)^n$:

$$\rho_c(\mathcal{C}, J) := \frac{1}{m}(\dim(\mathcal{C}) - \dim(\mathcal{C}(J^\perp, c)))$$

For $K \leq (\mathbb{F}_q)^m$:

$$\rho_r(\mathcal{C}, K) := \frac{1}{n}(\dim(\mathcal{C}) - \dim(\mathcal{C}(K^\perp, r)))$$

The two q-polymatroids associated to a MRMC

Let $\mathcal{C} \leq M_{n,m}(\mathbb{F}_q)$ MRMC

$P(\mathcal{C}, c) := ((\mathbb{F}_q)^n, \rho_c)$, $P(\mathcal{C}, r) := ((\mathbb{F}_q)^n, \rho_r)$ are q-polymatroids.

Why q-polymatroids?

GJLR

We can study properties of our code using q-polymatroids.

$\mathcal{C} \leq M_{n,m}(\mathbb{F}_q)$ MRMC

$$\dim(\mathcal{C}) = m\rho_c(\mathcal{C}, (\mathbb{F}_q)^n) = n\rho_r(\mathcal{C}, \mathbb{F}_{q^m})$$

GJLR

$\mathcal{C} \leq M_{n,m}(\mathbb{F}_q)$ nonzero MRMC.

TFAE

- $d(\mathcal{C}) \geq d$;
- $\rho_c(J) = \frac{\dim(\mathcal{C})}{m}$ for each $J \leq (\mathbb{F}_q)^n$ s.t. $\dim(J) \geq n - d + 1$;
- $\rho_r(K) = \frac{\dim(\mathcal{C})}{n}$ for each $K \leq (\mathbb{F}_q)^m$ s.t. $\dim(K) \geq m - d + 1$;

GJLR

So therefore...

$$d(\mathcal{C}) = n + 1 - \min\{d : \rho_c(J) = \dim(\mathcal{C})/m \text{ for each } J \leq (\mathbb{F}_q)^n \text{ s.t. } \dim(J) = d\}$$

$$d(\mathcal{C}) = m + 1 - \min\{d : \rho_r(K) = \dim(\mathcal{C})/n \text{ for each } K \leq (\mathbb{F}_q)^m \text{ s.t. } \dim(K) = d\}$$

MRD and rank

GJLR

$\mathcal{C} \leq M_{n,m}(\mathbb{F}_q)$ nonzero MRMC of minimum distance d

TFAE

- $\mathcal{C}$ MRD
- $\rho_c(J) = \dim(J)$, for each $J \leq (\mathbb{F}_q)^n$ s.t. $\dim(J) \leq n - d + 1$;
- $\rho_c(J) = \dim(J)$, for each $J \leq (\mathbb{F}_q)^n$ s.t. $\dim(J) = n - d + 1$;

MRD AND RANK

GJLR

$\mathcal{C} \leq M_{n,m}(\mathbb{F}_q)$ nonzero MRD of minimum distance d

For all $J \leq (\mathbb{F}_q)^n$:

$$\rho_c(J) = \begin{cases} n - d + 1 & \dim(J) \geq n - d + 1 \\ \dim(J) & \dim(J) \leq n - d + 1 \end{cases}$$

So we get a uniform q-matroid.

What happens with equivalence?

GJLR

$\mathcal{C}_1, \mathcal{C}_2 \leq M_{n,m}(\mathbb{F}_q)$ MRMC which are equivalent.

$m > n$

$$P(\mathcal{C}_1, c) \sim P(\mathcal{C}_2, c)$$
$$P(\mathcal{C}_1, r) \sim P(\mathcal{C}_2, r)$$

$m = n$

$$P(\mathcal{C}_1, c) \sim P(\mathcal{C}_2, c) \qquad P(\mathcal{C}_1, c) \sim P(\mathcal{C}_2, r)$$
$$P(\mathcal{C}_1, r) \sim P(\mathcal{C}_2, r) \quad \text{or} \quad P(\mathcal{C}_1, r) \sim P(\mathcal{C}_2, c)$$

But codes that are not equivalent can have the same or, in any case equivalent, q-polymatroids.

Back to q-matroids

JP-GJLR

As we know, a VRMC $C \leq (\mathbb{F}_{q^m})^n$ gives a q-matroid on $(\mathbb{F}_q)^n$.
If Γ is a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, $M_C = P(\Gamma(C), c)$.

GJLR

Let now Γ, Γ' be two bases of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$:

$$P(\Gamma(C), c) = P(\Gamma'(C), c)$$
$$P(\Gamma(C), r) \sim P(\Gamma'(C), r)$$

Warning

GJLR

There are examples of RMCs, whose associated *q*-polymatroids are not *q*-matroids...

... not even taking multiples of the rank.

GJLR

$\mathcal{C} \leq M_{n,m}(\mathbb{F}_q)$ nonzero MRMC.
Take an integer $1 \leq i \leq \dim(\mathcal{C})$.

$n < m$

$$w_i(\mathcal{C}) = \min\{n - \dim(J) : J \leq (\mathbb{F}_q)^n, \dim(\mathcal{C}) - m\rho_c(\mathcal{C}, J) \geq i\}$$

GJLR

$\mathcal{C} \leq M_{n,m}(\mathbb{F}_q)$ nonzero MRMC.
Take an integer $1 \leq i \leq \dim(\mathcal{C})$.

$n = m$

$$w_i(\mathcal{C}) = \min\{w_i(\mathcal{C}, c), w_i(\mathcal{C}, r)\}$$

$$w_i(\mathcal{C}, c) = \min\{n - \dim(J) : J \leq (\mathbb{F}_q)^n, \dim(\mathcal{C}) - m\rho_c(\mathcal{C}, J) \geq i\}$$
$$w_i(\mathcal{C}, r) = \min\{m - \dim(K) : K \leq (\mathbb{F}_q)^m, \dim(\mathcal{C}) - n\rho_r(\mathcal{C}, K) \geq i\}$$

GJLR

$\mathcal{C} \leq M_{n,m}(\mathbb{F}_q)$ MRMC.
$t = maxr(\mathcal{C})$.

TFAE

- $\mathcal{C}$ optimal anticode;
- $\{\rho_c(\mathcal{C}, J) : J \leq (\mathbb{F}_q)^n\} = \{0, ..., t\}$ or $\{\rho_r(\mathcal{C}, J) : J \leq (\mathbb{F}_q)^n\} = \{0, ..., t\}$, and $m = n$;
- $\rho_c(\mathcal{C}, (\mathbb{F}_q)^n) = t$ or $\rho_r(\mathcal{C}, (\mathbb{F}_q)^n) = t$ and $m = n$.

GJLR

$\mathcal{C} \leq M_{n,m}(\mathbb{F}_q)$ optimal anticode.
$t = maxr(\mathcal{C})$.

$m > n$

$$P(\mathcal{C}, c) \sim ((\mathbb{F}_q)^n, \rho)$$

with

$$\rho(J) = \dim(J + \langle \overline{\mathbf{e}}_1, ..., \overline{\mathbf{e}}_{n-t} \rangle) - (n - t)$$

GJLR

$\mathcal{C} \leq M_{n,m}(\mathbb{F}_q)$ optimal anticode.
$t = maxr(\mathcal{C})$.

$m = n$

$$P(\mathcal{C}, c) \sim ((\mathbb{F}_q)^n, \rho)$$

or

$$P(\mathcal{C}, r) \sim ((\mathbb{F}_q)^n, \rho)$$

Generalized weights and q-polymatroids (GJLR)

There are **some cases** in which the generalized weight determine $P(\mathcal{C}, c)$, up to equivalence.

Generalized weights of MRD $\Rightarrow$ MRD $+$ uniform q-matroid

Generalized weights of optimal anticode $\Rightarrow$ optimal anticode $+$ the q-matroid we just described.

There are **some cases** in which the generalized weight determine $P(\mathcal{C}, c)$, up to equivalence.

$\dim(\mathcal{C}) = 1$ so $\mathcal{C} = \langle A \rangle$.
$w_1(\mathcal{C}) = d = r(A)$

$$\rho_c(\mathcal{C}, J) = \begin{cases} 0 & colsp(A) \leq J^{\perp} \\ \frac{1}{m} & \text{otherwise} \end{cases}$$

Duality (MRMC)

GJLR

$\mathcal{C} \leq M_{n,m}(\mathbb{F}_q)$ MRMC

$$P(\mathcal{C}, c)^* = P(\mathcal{C}^\perp, c) \text{ and } P(\mathcal{C}, r)^* = P(\mathcal{C}^\perp, r)$$

Duality (VRMC)

GJLR

Let $C \leq (\mathbb{F}_{q^m})^n$ be a VRMC and Γ a basis of $\mathbb{F}_{q^m}$ over $\mathbb{F}_q$, whose dual basis is Γ^*. Let $\perp\!\!\!\perp$ be the standard inner product in $(\mathbb{F}_{q^m})^n$.

$$P(\Gamma(C^{\perp\!\!\!\perp}), c) = P(\Gamma^*(C), c) = P(\Gamma(C), c)^*$$
$$P(\Gamma(C^{\perp\!\!\!\perp}), r) = P(\Gamma^*(C), r) \sim P(\Gamma(C), r)^*.$$

Thank you for your attention!