Rank-metric codes and q-polymatroids

Relinde Jurrius

joint work with Elisa Gorla, Hiram López, Alberto Ravagnani

Netherlands Defence Academy

Combinatorics
June 5, 2018

Matroid: a pair (E, r) with

- E finite set;
- $r : 2^E \to \mathbb{N}_0$ a function, the *rank function*, with 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) $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$ (semimodular)

Independent set: $r(A) = |A|$

Example

$$\begin{pmatrix} 0 & 0 & 0 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 \end{pmatrix}$$

Fact: a linear code gives a matroid with

$E =$ index set for columns of generator matrix

$r(J) =$ dimension of subspace spanned by vectors of J

q-Analogues

Finite set $\longrightarrow$ finite dimensional vectorspace over $\mathbb{F}_q$

Example

$\binom{n}{k}$ = number of sets of size k contained in set of size n

$\begin{bmatrix} n \\ k \end{bmatrix}_q$ = number of k-dim subspaces of n-dim vectorspace over $\mathbb{F}_q$

finite set	finite space $\mathbb{F}_q^n$
element	1-dim subspace
size	dimension
n	$\frac{q^n-1}{q-1}$
intersection	intersection
union	sum

From q-analogue to 'normal': let $q \to 1$.

q-Matroid: a pair (E, r) with

- E finite dimensional vector space;
- $r : \{\text{subspaces of } E\} \to \mathbb{N}_0$ a function, the *rank function*, with for all $A, B \subseteq E$:

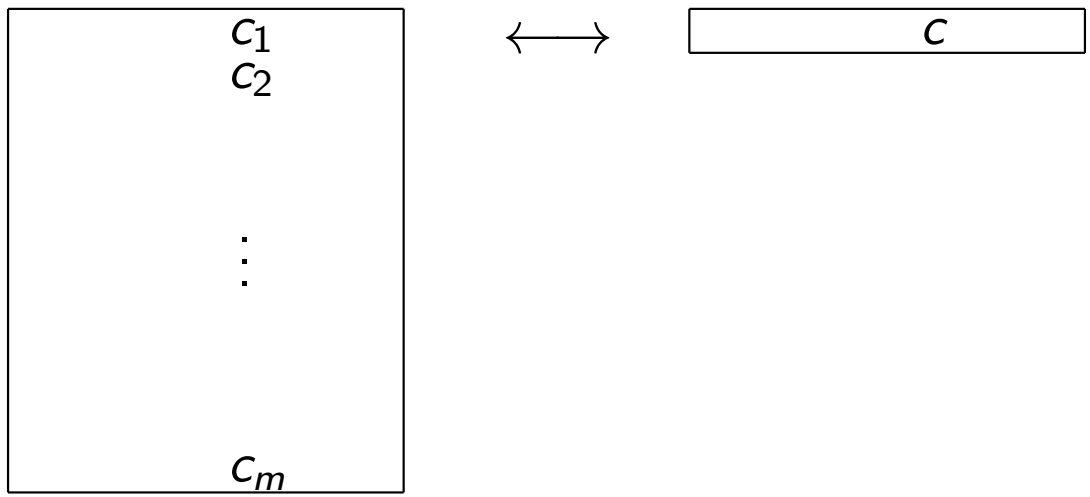
  (r1) $0 \leq r(A) \leq \dim A$
  (r2) If $A \subseteq B$ then $r(A) \leq r(B)$.
  (r3) $r(A + B) + r(A \cap B) \leq r(A) + r(B)$ (semimodular)

Matrix rank-metric code: subspace of $\mathbb{F}_q^{m\times n}$.

Vector rank-metric code: subspace of $\mathbb{F}_{q^m}^n$

$\mathbb{F}_{q^m}/\mathbb{F}_q$ finite field extension with basis $\alpha_1, \ldots, \alpha_m$.

Write $c = c_1\alpha_1 + \cdots + c_m\alpha_m$.



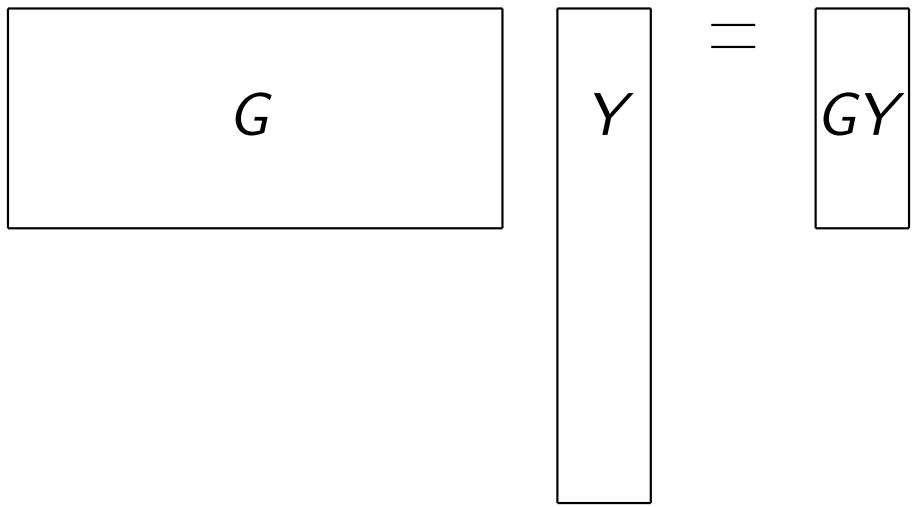
$m(\mathbf{x}) \in \mathbb{F}_q^{m\times n}$ $\qquad$ $\mathbf{x} \in \mathbb{F}_{q^m}^n$

Theorem (J. & Pellikaan, 2016)

Every vector rank-metric code gives a q-matroid.

Proof.

Let $E = \mathbb{F}_q^n$ and G be a generator matrix of the code.
Let $A \subseteq E$ and Y a matrix whose columns span A.



Then $r(A) = \mathrm{rk}(GY)$ satisfies the axioms (r1),(r2),(r3). $\square$

What about matrix rank-metric codes?

Theorem (Vector rank-metric code)

Let $\ell(J) = \dim\{\mathbf{c} \in C : \mathit{rowsp}(m(\mathbf{c})) \subseteq J^{\perp}\}$. *Then*

$$r(J) = \dim C - \ell(J).$$

Definition (Matrix rank-metric code)

$\ell(J) = \dim\{M \in C : \mathrm{rowsp}(M) \subseteq J^{\perp}\}, \quad \rho(J) = \frac{1}{m}(\dim C - \ell(J))$

Polymatroid: a pair (E, ρ) with

- E finite set;
- $\rho : 2^E \to \mathbb{R}$ a function, the *rank function*, with for all $A, B \in E$:

  (P1) $\rho(\emptyset) = 0$
  (P2) If $A \subseteq B$ then $\rho(A) \leq \rho(B)$.
  (P3) $\rho(A \cup B) + \rho(A \cap B) \leq \rho(A) + \rho(B)$ (semimodular)

q-Polymatroid: a pair (E, ρ) with

- E finite dimensional vector space;
- $\rho : \{\text{subspaces of } E\} \to \mathbb{R}$ a function, the *rank function*, with for all $A, B \subseteq E$:

  (P1) $\rho(\mathbf{0}) = 0$
  (P2) If $A \subseteq B$ then $\rho(A) \leq \rho(B)$.
  (P3) $\rho(A + B) + \rho(A \cap B) \leq \rho(A) + \rho(B)$ (semimodular)

We assume $\rho(x) \leq 1$ for all 1-dim subspaces $x \subseteq E$.

Theorem (Gorla, J., López, Ravagnani, 2018)

Every matrix rank-metric code gives a q-polymatroid, that is, $\rho(J) = \frac{1}{m}\left(\dim C - \ell(J)\right)$ *satisfies (P1),(P2),(P3).*

The code is a vector rank-metric code iff we get a q-matroid.

Invariants of rank-metric codes defined by q-polymatroid:

- *minimum distance & being MRD,*
- *generalized weights & optimal anticodes,*
- *duality.*