Defining the q-analogue of a matroid

Relinde Jurrius
(joint work with Ruud Pellikaan)

Université de Neuchâtel, Switzerland

Aalto University
February 10, 2016

Matroid: a pair $(E, \mathcal{I})$ with

- E finite set;
- $\mathcal{I} \subseteq 2^E$ family of subsets of E, the *independent sets*, with:
  (I1) $\emptyset \in \mathcal{I}$
  (I2) If $A \in \mathcal{I}$ and $B \subseteq A$ then $B \in \mathcal{I}$.
  (I3) If $A, B \in \mathcal{I}$ and $|A| > |B|$ then there is an $a \in A \setminus B$ such that $B \cup \{a\} \in \mathcal{I}$.

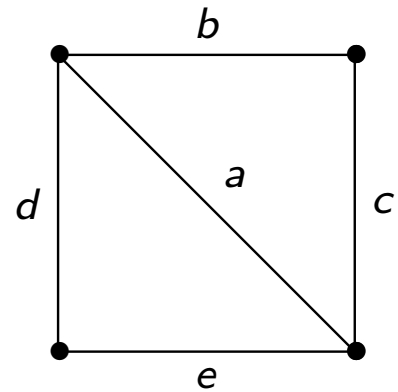
Examples:

- Set of vectors; independence = linear independence
- Set of edges of a graph; independence = cycle free

Example

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

Example



But: most matroids don't come from a matrix or graph.

A matroid is also 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)

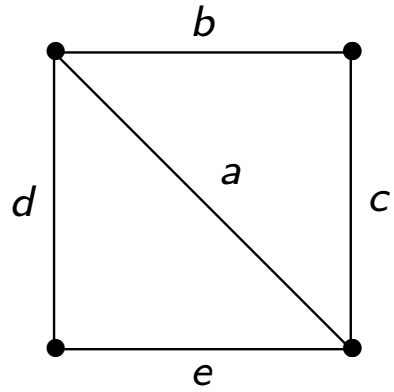
$r(A) =$ size of largest independent set contained in A

$\mathcal{I} = \{$subsets whose size is equal to their rank$\}$

Example

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

Example



Basis: maximal independent set wrt inclusion

All bases have the same size.

Loop: element that is in no independent set (i.e., $r(x) = 0$)

Rank of M: rank of the ground set E

q-Analogues

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

Example

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

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

$$= \prod_{i=0}^{k-1} \frac{q^n - q^i}{q^k - q^i}$$

q-Analogues

Example

t-(v, k, λ) design: pair $(X, \mathcal{B})$ with

- X set with v elements (points)
- $\mathcal{B}$ family of subsets of X of size k (blocks)
- Every t-tuple of points is contained in exactly λ blocks

t-$(v, k, \lambda; q)$ q-design: pair $(X, \mathcal{B})$ with

- X v-dim vectorspace over $\mathbb{F}_q$
- $\mathcal{B}$ family of k-dim subspaces of X (blocks)
- Every t-dim subspace is contained in exactly λ blocks

q-Analogues

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
complement	?

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

Candidates for complement A^c of $A \subseteq \mathbb{F}_q^n$:

- All vectors outside A
  But: not a space
- Orthogonal complement
  But: $A \cap A^\perp$ can be nontrivial
- Quotient space $\mathbb{F}_q^n / A$
  But: changes ambient space
- Subspace such that $A \oplus A^c = \mathbb{F}_q^n$
  But: not unique

Linear codes

A linear code C is a subspace of $\mathbb{F}_q^n$.

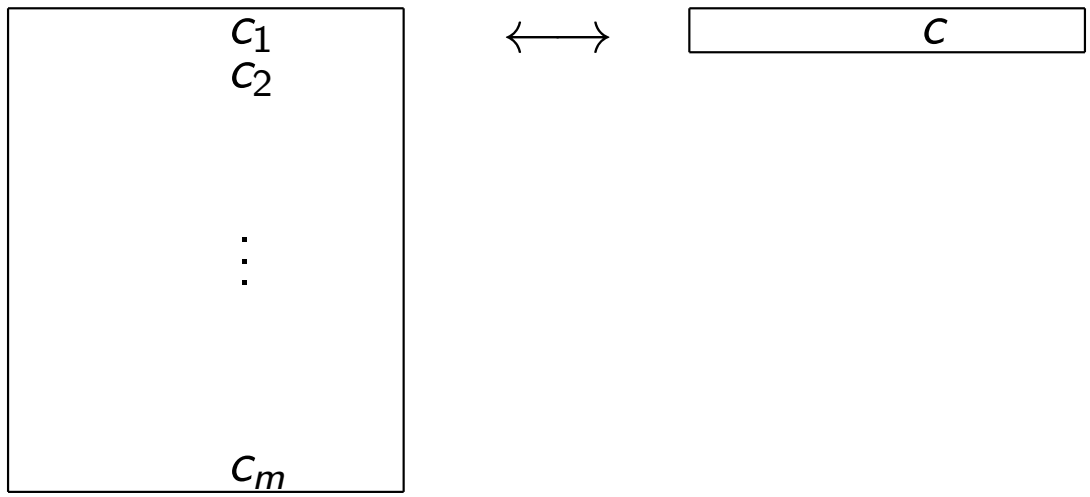
- n length of the code
- k dimension of the code

A $k \times n$ matrix whose rows span C is called a generator matrix.

Rank metric codes

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

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



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

Rank metric code is subspace of $\mathbb{F}_{q^m}^n \to$ subspace of $\mathbb{F}_q^{m\times n}$.

Running example

Let $\mathbb{F}_8/\mathbb{F}_2$ with basis $(1, \alpha, \alpha^2)$, where $\alpha^3 = \alpha + 1$.
Let C be the code generated by

$$G = \begin{pmatrix} 1 & \alpha & 0 & 0 \\ 0 & 1 & \alpha & 0 \end{pmatrix}.$$

Some words and matrices:

$\mathbf{c}$	$(0,0,0,0)$	$(1,\alpha,0,0)$	$(1,\alpha^2,\alpha^5,0)$
$m(\mathbf{c})$	$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}$

C linear code

$\mathrm{supp}(\mathbf{c}) =$ coordinates of $\mathbf{c}$ that are non-zero

$\mathrm{wt}_H(\mathbf{c}) =$ size of support

Weight enumerator

$$W_C(X, Y) = \sum_{w=0}^{n} A_w X^{n-w} Y^w$$

with $A_w =$ number of words of weight w.

C rank metric code

$\mathrm{Rsupp}(\mathbf{c}) =$ row space of $m(\mathbf{c})$

$\mathrm{wt}_R(\mathbf{c}) =$ dimension of support

Rank weight enumerator

$$W_C^R(X, Y) = \sum_{w=0}^{n} A_w^R X^{n-w} Y^w$$

with $A_w^R =$ number of words of rank weight w.

Example

C in $\mathbb{F}_8/\mathbb{F}_2$ generated by $G = \begin{pmatrix} 1 & \alpha & 0 & 0 \\ 0 & 1 & \alpha & 0 \end{pmatrix}$.

Some words and weights:

$\mathbf{c}$	$(0,0,0,0)$	$(1,\alpha,0,0)$	$(1,\alpha^2,\alpha^5,0)$
$m(\mathbf{c})$	$\begin{pmatrix} 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$	$\begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 \end{pmatrix}$
Rsupp($\mathbf{c}$)	$\mathbf{0}$	$\left\langle \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{pmatrix} \right\rangle$	$\left\langle \begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{pmatrix} \right\rangle$
$\mathrm{wt}_R(\mathbf{c})$	0	2	3

There are no words of weight 1 or weight 4.

J subset of $[n]$

$$C(J) = \{\mathbf{c} \in C : \mathrm{supp}(\mathbf{c}) \subseteq J^c\}$$

Lemma
$C(J)$ is a subspace of $\mathbb{F}_q^n$

$$\ell(J) = \dim_{\mathbb{F}_q} C(J)$$

Theorem
$\ell(J)$ gives a nice formula for the weight enumerator.

J subspace of $\mathbb{F}_q^n$

$$C(J) = \{\mathbf{c} \in C : \mathrm{Rsupp}(\mathbf{c}) \subseteq J^{\perp}\}$$

Lemma
$C(J)$ is a subspace of $\mathbb{F}_{q^m}^n$

$$\ell(J) = \dim_{\mathbb{F}_{q^m}} C(J)$$

Theorem
$\ell(J)$ gives a nice formula for the rank weight enumerator.

Example

C in $\mathbb{F}_8/\mathbb{F}_2$ generated by $G = \begin{pmatrix} 1 & \alpha & 0 & 0 \\ 0 & 1 & \alpha & 0 \end{pmatrix}$.

Some calculations of $C(J)$:

J	$J^\perp$	$C(J)$
$\mathbb{F}_2^4$	$\mathbf{0}$	$\mathbf{0}$
$\dim = 3$	$\dim = 1$	$\mathbf{0}$
$\left\langle \begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{matrix} \right\rangle$	$\left\langle \begin{matrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{matrix} \right\rangle$	$\mathbf{0}$
$\left\langle \begin{matrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{matrix} \right\rangle$	$\left\langle \begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{matrix} \right\rangle$	$\left\langle \begin{matrix} 1 & \alpha & 0 & 0 \end{matrix} \right\rangle$

If $\dim J = 2$ and $J^\perp \not\subseteq \left\langle \begin{matrix} 0 & 0 & 0 & 1 \end{matrix} \right\rangle^\perp$ then $C(J) = \mathbf{0}$.

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

Theorem

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

Idea of proof: $0 \to C(J) \to C \to C_J \to 0$ is an exact sequence.

Corollary

The Tutte polynomial of a matroid determines the (extended) weight enumerator of the corresponding code, via $\ell(J)$.

ULTIMATE GOAL: Find a q-analogue of this correspondence.

(Break)

Matroid: a pair $(E, \mathcal{I})$ with

- E finite set;
- $\mathcal{I} \subseteq 2^E$ family of subsets of E, the *independent sets*, with:
  (I1) $\emptyset \in \mathcal{I}$
  (I2) If $A \in \mathcal{I}$ and $B \subseteq A$ then $B \in \mathcal{I}$.
  (I3) If $A, B \in \mathcal{I}$ and $|A| > |B|$ then there is an $a \in A \setminus B$ such that $B \cup \{a\} \in \mathcal{I}$.

Examples:

- Set of vectors; independence = linear independence
- Set of edges of a graph; independence = cycle free

A matroid is also 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)

$r(A) =$ size of largest independent set contained in A

$\mathcal{I} = \{$subsets whose size is equal to their rank$\}$

q-Analogues

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
complement	(it depends)

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

q-Matroid: a pair $(E, \mathcal{I})$ with

- E finite dimensional vector space;
- $\mathcal{I}$ family of subspaces of E, the *independent spaces*, with:

  (I1) $\mathbf{0} \in \mathcal{I}$

  (I2) If $A \in \mathcal{I}$ and $B \subseteq A$ then $B \in \mathcal{I}$.

  (I3) If $A, B \in \mathcal{I}$ and $\dim A > \dim B$ then there is a 1-dimensional subspace $a \subseteq A$, $a \nsubseteq B$ such that $B + a \in \mathcal{I}$.

A q-matroid could also be 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)

$r(A) =$ dimension of largest independent space contained in A

$\mathcal{I} = \{\text{subspaces whose dimension is equal to their rank}\}$

Recall: $\ell(J) = \dim C(J) = \dim\{\mathbf{c} \in C : \mathrm{Rsupp}(\mathbf{c}) \subseteq J^{\perp}\}$

Theorem
Let $r(J) = \dim C - \ell(J)$ for a rank metric code C. Then $r(J)$ is the rank function of a q-matroid, i.e., r satisfies (r1),(r2),(r3).

Again, there is an exact sequence $0 \to C(J) \to C \to C_J \to 0$.

Example

C in $\mathbb{F}_8/\mathbb{F}_2$ generated by $G = \begin{pmatrix} 1 & \alpha & 0 & 0 \\ 0 & 1 & \alpha & 0 \end{pmatrix}$.

Some calculations of $r(J)$:

J	$C(J)$	$r(J)$
$\mathbb{F}_2^4$	$\mathbf{0}$	2
$\dim = 3$	$\mathbf{0}$	2
$\left\langle \begin{matrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{matrix} \right\rangle$	$\mathbf{0}$	2
$\left\langle \begin{matrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{matrix} \right\rangle$	$\langle \begin{matrix} 1 & \alpha & 0 & 0 \end{matrix} \rangle$	1

If $\dim J = 2$ and $J^\perp \not\subseteq \langle \begin{matrix} 0 & 0 & 0 & 1 \end{matrix} \rangle^\perp$ then $r(J) = 2$.

These are exactly the bases of the q-matroid.

Lemma

Let $\dim J = t$. *Then*

$$\ell(J) = \begin{cases} k - t & \text{for all } t < d^{\perp} \\ 0 & \text{for all } t > n - d \end{cases}$$

Corollary

MRD codes have $d = n - k + 1$ *and* $d^{\perp} = k + 1$.
Hence the associated q-matroid has rank function

$$r(J) = \begin{cases} t & \text{for all } t \leq k \\ k & \text{for all } t > k \end{cases}.$$

This is called the uniform q-matroid $U_{k,n}$.

Example

Let $E = \mathbb{F}_2^4$ and $\mathcal{I} = \left\{ \left\langle \begin{array}{cccc} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{array} \right\rangle \text{ and all its subspaces} \right\}$.

$\mathcal{I}$ satisfies (I1),(I2),(I3), and r satisfies (r1),(r2). But:

$$A = \left\langle \begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{array} \right\rangle \quad B = \left\langle \begin{array}{cccc} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right\rangle$$

Then $r(A+B) + r(A \cap B) = 2 + 1 > 1 + 1 = r(A) + r(B)$!

Problem: (r1),(r2),(r3) $\Rightarrow$ (I1),(I2),(I3); but not $\Leftarrow$.

Possible solutions:

- Keep (I1),(I2),(I3) and find "relaxation" of (r3).
- Keep (r1),(r2),(r3) and find extra axiom for $\mathcal{I}$.

New matroids from old

Let M a matroid on E with $|E| = n$ and $r(M) = k$.

- Duality: $[n, n-k]$
- Deletion: $[n-1, k]$
- Contraction: $[n-1, k-1]$
- First deletion, then duality = first duality, then contraction

q-analogue of these constructions?

New q-matroids from old

- Deletion $[n-1, k]$ and contraction $[n-1, k-1]$
  - Definition and proof in terms of rank function
  - Also in terms of independent spaces
- Duality $[n, n-k]$
  - Definition and proof in terms of rank function
    $\Rightarrow$ dual bases are orthogonal complements of bases
  - No clue how to prove it using independent spaces
  - Coincides with duality in rank metric codes
- First deletion, then duality = first duality, then contraction
  - Proven: bases are the same

Problem: (r1),(r2),(r3) $\Rightarrow$ (I1),(I2),(I3); but not $\Leftarrow$.

Possible solutions:

1. Keep (I1),(I2),(I3) and find "relaxation" of (r3).
2. Keep (r1),(r2),(r3) and find extra axiom for $\mathcal{I}$.

Conclusion: solution 2.

Example

Let $E = \mathbb{F}_2^4$ and $\mathcal{I} = \left\{ \left\langle \begin{array}{cccc} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{array} \right\rangle \text{ and all its subspaces} \right\}$.

$\mathcal{I}$ satisfies (I1),(I2),(I3), and r satisfies (r1),(r2). But:

$$A = \left\langle \begin{array}{cccc} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{array} \right\rangle \quad B = \left\langle \begin{array}{cccc} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{array} \right\rangle$$

Then $r(A + B) + r(A \cap B) = 2 + 1 > 1 + 1 = r(A) + r(B)$.

Possible new axiom: (I0) $\mathrm{span}(\mathcal{I}) = E$.

Does this mean no loops allowed? No:

Example

C in $\mathbb{F}_8/\mathbb{F}_2$ generated by $G = \begin{pmatrix} 1 & \alpha & 0 & 0 \\ 0 & 1 & \alpha & 0 \end{pmatrix}$.

If $\dim J = 2$ and $J^\perp \not\subseteq \left\langle \begin{array}{cccc} 0 & 0 & 0 & 1 \end{array} \right\rangle^\perp$ then $r(J) = 2$.

So the bases are exactly the 2-dim subspaces that do not contain $\left\langle \begin{array}{cccc} 0 & 0 & 0 & 1 \end{array} \right\rangle$. They span E.

Lemma
Let $A \subseteq E$ and I a maximal independent subspace of A.
Let $x \subseteq E$ a 1-dim subspace.
Then $I + x$ contains a maximal independent subspace of $A + x$.

Proven: (I1),(I2),(I3) + Lemma $\Rightarrow$ (r1),(r2),(r3)

To do:

- Prove (I0),(I1),(I2),(I3) $\Rightarrow$ Lemma
- Prove (r1),(r2),(r3) $\Rightarrow$ (I0)

What's next?

Right now:

- Prove (I0) suffices (or find a different solution)

Soon:

- More cryptomorphic descriptions (bases, circuits, flats, . . .)

What's next?

Dots on the horizon:

- q-analogue of Tutte polynomial
- Link with rank weight enumerator
- Rank metric codes that are not $\mathbb{F}_{q^m}$-linear
- Link with other q-analogues?
- Do all q-matroids come from rank metric codes?
- Is a q-matroid a matroid over a hyperfield?

Thank you for your attention.