Defining the q-analogue of a matroid

Relinde Jurrius
(joint work with Ruud Pellikaan)

Université de Neuchâtel, Switzerland

Network Coding and Designs
April 5, 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

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$\}$

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

The Tutte polynomial of a matroid determines the (extended) weight enumerator of the corresponding code.

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

q-Analogues

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

Example

$$
\begin{aligned}
\binom{n}{k} &= \text{number of sets of size } k \text{ contained in set of size } n \\
\begin{bmatrix} n \\ k \end{bmatrix}_q &= \text{number of } k\text{-dim subspaces of } n\text{-dim vectorspace over } \mathbb{F}_q \\
&= \prod_{i=0}^{k-1} \frac{q^n - q^i}{q^k - q^i}
\end{aligned}
$$

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

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 $a \subseteq A$, $a \not\subseteq B$ 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

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

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

Necessary condition

Possible new axiom:

(I4) For all $A \subseteq E$, span$\{I \in \mathcal{I} : I \subseteq A\}$ is either $\mathbf{0}$ or A.

Proven: (r1),(r2),(r3) $\Rightarrow$ (I4)

Sufficient condition

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: (I1),(I2),(I3),(I4) $\Rightarrow$ Lemma

What's next?

Right now:

- Prove (I4) 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?

Thank you for your attention.