Defining the $q$-analogue of a matroid

Relinde Jurrius
(joint work with Ruud Pellikaan)

Université de Neuchâtel, Switzerland

Workshop on structure in graphs and matroids
July 29, 2016
\textit{q-Analogues}

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

Example

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

\[
\left[ \begin{array}{c} n \\ k \end{array} \right]_q = \text{number of } k\text{-dim subspaces of } n\text{-dim vectorspace over } \mathbb{F}_q
\]

\[
= \prod_{i=0}^{k-1} \frac{q^n - q^i}{q^k - q^i}
\]
\( q \)-Analogues

<table>
<thead>
<tr>
<th>finite set</th>
<th>finite space ( \mathbb{F}_q^n )</th>
</tr>
</thead>
<tbody>
<tr>
<td>element</td>
<td>1-dim subspace</td>
</tr>
<tr>
<td>size</td>
<td>dimension</td>
</tr>
<tr>
<td>( n )</td>
<td>( \frac{q^n-1}{q-1} )</td>
</tr>
<tr>
<td>intersection</td>
<td>intersection</td>
</tr>
<tr>
<td>union</td>
<td>sum</td>
</tr>
<tr>
<td>complement</td>
<td>?</td>
</tr>
</tbody>
</table>

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
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.

Hamming distance: $d(x, y) = |\{i \in [n] : x_i \neq y_i\}|$. 
Idea: send (rows of) matrices instead of vectors

[Other idea: send (bases of) subspaces instead of matrices]
Rank metric codes

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

Write \( c = c_1 \alpha_1 + \cdots + c_m \alpha_m \).

\[
\begin{array}{c}
c_1 \\
c_2 \\
\vdots \\
c_m
\end{array}
\longleftrightarrow
\begin{array}{c}
\hspace{5em} \mathbf{c} \hspace{5em}
\end{array}
\]

\[ m(\mathbf{x}) \in \mathbb{F}_q^{m \times n} \quad \mathbf{x} \in \mathbb{F}_{q^m}^n \]

**Rank metric code** is subspace of \( \mathbb{F}_{q^m}^n \rightarrow \) subspace of \( \mathbb{F}_q^{m \times n} \).

Rank distance: \( d(A, B) = \text{rk}(A - B) \)
C linear code

\[ \text{supp}(\mathbf{c}) = \text{coordinates of } \mathbf{c} \text{ that are non-zero} \]
\[ \text{wt}_H(\mathbf{c}) = \text{size of support} \]

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

\[ \text{Rsupp}(c) = \text{row space of } m(c) \]
\[ \text{wt}_R(c) = \text{dimension of support} \]

Rank weight enumerator

\[ W_C^R(X, Y) = \sum_{w=0}^{n} A^R_w X^{n-w} Y^w \]

with \( A^R_w = \text{number of words of rank weight } w. \)
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.
Lemma

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

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

Theorem

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

$\ell(J)$ gives a nice formula for the rank weight enumerator.
A linear code is a matroid, represented by a generator matrix.

**Theorem**

\[ \ell(J) = \dim C - r(J) \]

**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.
Theorem
Let \( r(J) = \dim C - \ell(J) \) for a rank metric code \( C \). Then \( r(J) \) satisfies for all \( A, B \subseteq E \):

\[(r1) \ 0 \leq r(A) \leq \dim A \]

\[(r2) \text{ If } A \subseteq B \text{ then } r(A) \leq r(B). \]

\[(r3) \ r(A + B) + r(A \cap B) \leq r(A) + r(B) \]

**q-Matroid:** a pair \((E, r)\) with
- \( E \) finite dimensional vector space;
- \( r : \{\text{subspaces of } E\} \rightarrow \mathbb{N}_0 \) a function, the *rank function*, that satisfies (r1),(r2),(r3).
Let $e \subseteq E$ a 1-dimension subspace.

Restriction (or: deletion of $e$)

Ground space: hyperplane $e^\perp$

Rank: $r_{M-e}(A) = r_M(A)$

Contraction of $e$

Ground space: quotient $E/e$, with a projection $\pi : E \rightarrow E/e$

Rank: $r_{M/e}(A) = r_M(B) - 1$, with $B \subseteq E$ unique such that $e \subseteq B$ and $\pi(B) = A$
Duality

Ground space: $E$

Rank: $r_{M^*}(A) = r_M(A^\bot) + \dim A - r(M)$

$\Rightarrow$ Bases: orthogonal complements of bases of $M$

First deletion, then duality = first duality, then contraction
Independent spaces: \( \mathcal{I} = \{ I \subseteq E : r(I) = \dim I \} \)

**Theorem**

The independent spaces of a q-matroid satisfy:

(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 \( B + a \in \mathcal{I} \).

Opposite is not true...
Example

Let $E = \mathbb{F}_2^4$ and $\mathcal{I} = \left\{ \langle \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{bmatrix} \rangle \text{ and all its subspaces} \right\}$. $\mathcal{I}$ satisfies (l1),(l2),(l3), and $r$ satisfies (r1),(r2). But:

$$A = \langle \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \end{bmatrix} \rangle \quad B = \langle \begin{bmatrix} 0 & 0 & 0 & 1 \end{bmatrix} \rangle$$

Then $r(A + B) + r(A \cap B) = 2 + 0 > 1 + 0 = r(A) + r(B)$!
Problem: embedding $\mathcal{I}$ in a bigger space does not give a $q$-matroid.

Solution: extra axiom for independence.

(I4) Let $x \notin \mathcal{I}$, $A \subseteq E$ and $I$ a maximal independent space in $A$. Then $I + x$ is a maximal independent space in $A + x$.

Or: if $r(A) = r(A + x) = r(A + y)$, then $r(A) = r(A + x + y)$.

Theorem
Let $\mathcal{I}$ satisfy (I1)–(I4). Then $\mathcal{I}$ is the collection of independent spaces of a $q$-matroid.
What’s next?

- More cryptomorphic descriptions (bases, circuits, flats, \ldots)
- Define $q$-analogue of Tutte polynomial
- Link with rank weight enumerator
- Rank metric codes that are not $\mathbb{F}_{q^m}$-linear
- Link with puncturing/shortening of rank metric codes?
- Link with other $q$-analogues?
- Do all $q$-matroids come from rank metric codes?

- Pick your favorite matroid theorem and find a $q$-analogue!