The $q$-analogue of a matroid

Relinde Jurrius
(joint work with Guus Bollen, Henry Crapo, Ruud Pellikaan)

Université de Neuchâtel, Switzerland

Structure in Graphs and Matroids
July 18, 2017
$q$-Analogues

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

Example

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

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

$$= \prod_{i=0}^{k-1} \frac{q^n - q^i}{q^k - q^i}$$
### $q$-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>it depends</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
**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)
Theorem (J. & Pellikaan, 2016)

Every $\mathbb{F}_{q^m}$-linear 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 $A$.

\[ G \begin{array}{c} \text{Y} \end{array} = GY \]

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

Matrix representation is equivalent under

- row operations over $\mathbb{F}_{q^m}$;
- column operations over $\mathbb{F}_q$.

Conjecture (J. & Torielli, 2017)

All $q$-matroids come from rank metric codes.

That means: a $q$-matroid over $E = \mathbb{F}_q^n$ of rank $k$ can be represented by a $k \times n$ matrix over a suitably large extension field $\mathbb{F}_{q^m}$. 
A q-matroid could also be a pair \((E, \mathcal{I})\) with

- \(E\) finite dimensional vector space;
- \(\mathcal{I}\) family of subspaces of \(E\), the independent spaces, with:
  1. \(0 \in \mathcal{I}\).
  2. If \(J \in \mathcal{I}\) and \(I \subseteq J\), then \(I \in \mathcal{I}\).
  3. If \(I, J \in \mathcal{I}\) with \(\dim I < \dim J\), then there is some 1-dimensional subspace \(x \subseteq J\), \(x \not\subseteq I\) with \(I + x \in \mathcal{I}\).

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

\(\mathcal{I} = \) \{subspaces whose dimension is equal to their rank\}
Example

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

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

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

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

Then $r(A + B) + r(A \cap B) = 2 + 1 > 1 + 1 = r(A) + r(B)$.
Problem: \((r1),(r2),(r3) \Rightarrow (l1),(l2),(l3)\); but not \(\Leftarrow\).

Solution: find an extra axiom \((l4)\) for \(\mathcal{I}\)

Lemma

*Loops come in subspaces.*

Corollary

*If an axiom set is invariant under embedding \(E\) in a bigger space, it can not be a full axiom set for \(\mathcal{I}\).*
Theorem
A q-matroid is a pair \((E, \mathcal{I})\) with

- \(E\) finite dimensional vector space;
- \(\mathcal{I}\) family of subspaces of \(E\), the independent spaces, with:
  1. \(\mathcal{I} \neq \emptyset\).
  2. If \(J \in \mathcal{I}\) and \(I \subseteq J\), then \(I \in \mathcal{I}\).
  3. If \(I, J \in \mathcal{I}\) with \(\dim I < \dim J\), then there is some \(1\)-dimensional subspace \(x \subseteq J\), \(x \not\subseteq I\) with \(I + x \in \mathcal{I}\).
  4. Let \(A, B \subseteq E\) and let \(I, J\) be maximal independent subspaces of \(A\) and \(B\), respectively. Then there is a maximal independent subspace of \(A + B\) that is contained in \(I + J\).
Example

\[
\{a, b, c, d\}
\]

\[
\{a, b, c\} \quad \{a, b, d\} \quad \{a, c, d\} \quad \{b, c, d\}
\]

\[
\{a, b\} \quad \{a, c\} \quad \{a, d\} \quad \{b, c\} \quad \{b, d\} \quad \{c, d\}
\]

\[
\{a\} \quad \{b\} \quad \{c\} \quad \{d\}
\]

\[
\emptyset
\]
Matriod $\iff$ only the following diamonds:

```
\begin{array}{cccc}
\text{one} & \text{zero} & \text{mixed} & \text{prime} \\
\end{array}
```

$q$-analogue: change Boolean lattice to subspace lattice (or another complemented modular lattice)
$q$-Matriod $\iff$ only the following “diamonds”:

- **one**
- **zero**
- **mixed**
- **prime**
Example

Z 12
Example
Rank generating polynomial:

\[ R(x, y) = \sum_{A \subseteq E} x^{r(M) - r(A)} y^{\dim(A) - r(A)} \]

Tutte polynomial:

- **classical**: \( x \rightarrow x - 1, \ y \rightarrow y - 1 \)
- **q**: something similar but with powers of \( q \) ??
Original Tutte polynomial:

\[ T(x, y) = \sum_{B \in \mathcal{B}} x^{i(B)} y^{e(B)} \]

Internal/external activity uses ordering on elements of the matroid.

Ordering on 1-dimensional subspaces ??
Internal/external activity induces partition of lattice in prime-free minors; that gives the Tutte polynomial.

**classical**: every part contains a basis

**q**: several bases per part, what is the right partition?

So the $q$-Tutte polynomial is a sum over parts of the partition: exponents of $x$ and $y$ depend on rank/nullity of the parts.
Example

\[ T(x, y) = x^2 + xy + 3x \]
What’s next?

Work in progress:

- $q$-analogue of Tutte polynomial
- Link with rank weight enumerator
- Do all $q$-matroids come from rank metric codes? How?

Long term:

- More cryptomorphic descriptions (circuits, flats, closure, …)
- Rank metric codes that are not $\mathbb{F}_{q^m}$-linear
- Puncturing and shortening of rank metric codes vs. restriction and contraction of $q$-matroids?
- Link with other $q$-analogues?