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 $\longrightarrow$ 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	it depends

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 $r(A) \leq r(B)$.

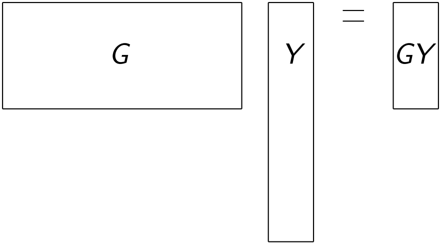
  (r3) $r(A + B) + r(A \cap B) \leq r(A) + r(B)$ (semimodular)

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.



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

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:
  - (I1) $\mathbf{0} \in \mathcal{I}$.
  - (I2) If $J \in \mathcal{I}$ and $I \subseteq J$, then $I \in \mathcal{I}$.
  - (I3) If $I, J \in \mathcal{I}$ with $\dim I < \dim J$, then there is some 1-dimensional subspace $x \subseteq J$, $x \nsubseteq I$ 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 $\mathcal{I} = \left\{ \left\langle \begin{array}{cccc} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{array} \right\rangle \text{ and all its subspaces} \right\}$.

$\mathcal{I}$ 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 $\Leftarrow$.

Solution: find an extra axiom (I4) for $\mathcal{I}$

Lemma

Loops come in subspaces.

Corollary

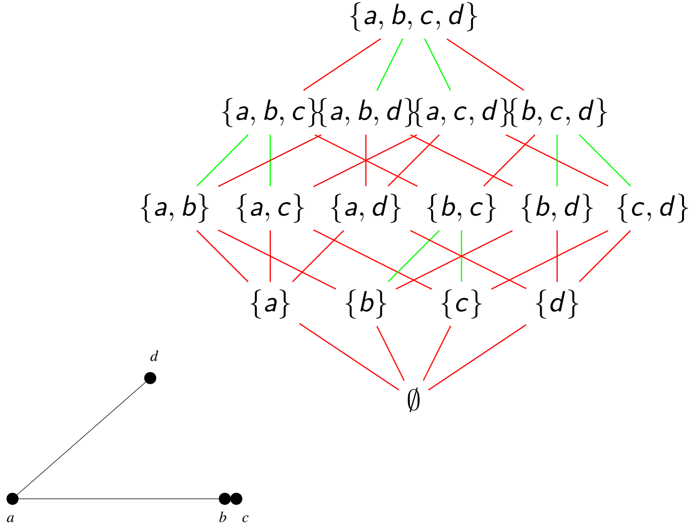
If an axiom set is invariant under embedding E in a bigger space, it can not be a full axiom set for $\mathcal{I}$.

Theorem

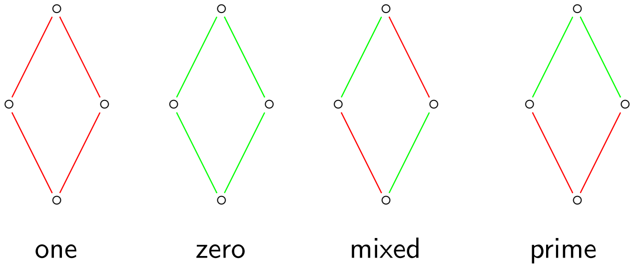
A q-matroid is a pair $(E, \mathcal{I})$ with

- *E finite dimensional vector space;*
- *$\mathcal{I}$ family of subspaces of E, the independent spaces, with:*
  - (I1) $\mathcal{I} \neq \emptyset$.
  - (I2) *If $J \in \mathcal{I}$ and $I \subseteq J$, then $I \in \mathcal{I}$.*
  - (I3) *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 $I + x \in \mathcal{I}$.*
  - (I4) *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

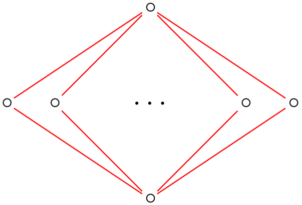


Matriod $\iff$ only the following diamonds:

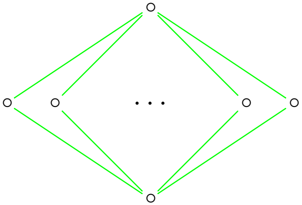


q-analogue: change Boolean lattice to subspace lattice
(or another complemented modular lattice)

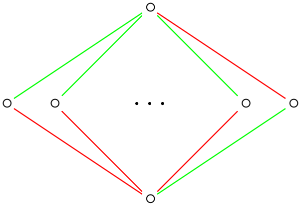
q-Matriod $\iff$ only the following "diamonds":



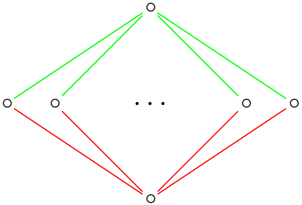
one



zero

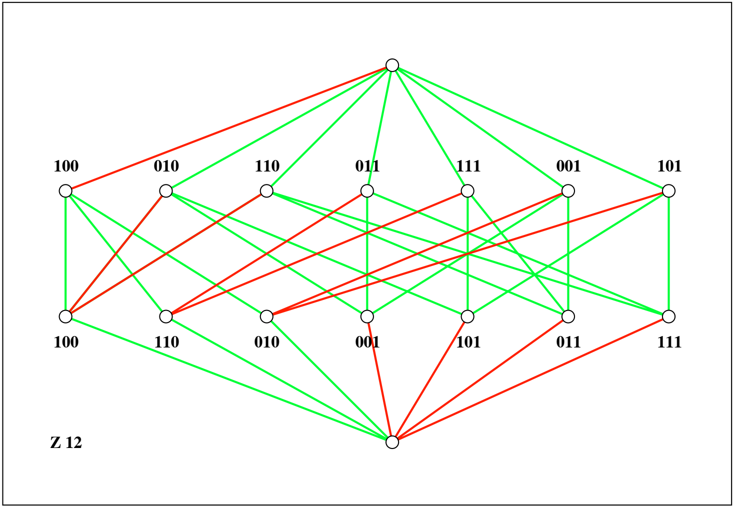


mixed

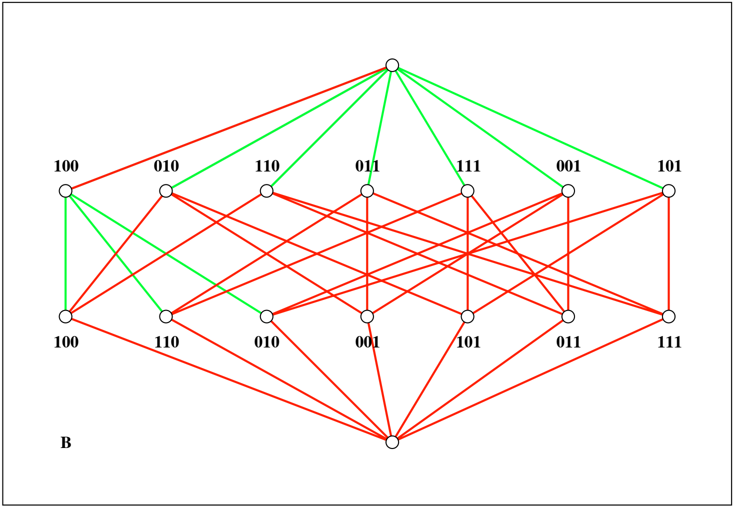


prime

Example



Example



Rank generating polynomial:

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

Tutte polynomial:

classical: $x \to x-1, \;\; y \to y-1$

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 ??

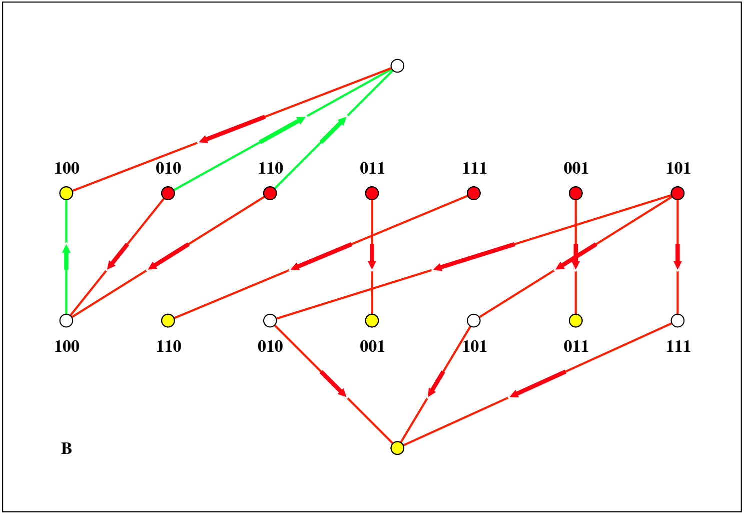
Internal/external activity induces partition of lattice in prime-free minors; that gives the Tutte polynomial.

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?