The q-analogue of matroids and their Tutte polynomial

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

Université de Neuchâtel, Switzerland
(→ The Netherlands Defence Academy)

InterCity seminar
November 3, 2017

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

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

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 $B \cup \{a\} \in \mathcal{I}$.

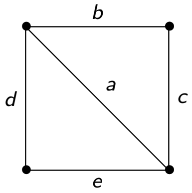
Examples:

- 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)

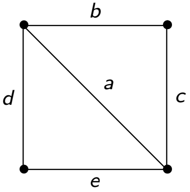
$r(A) =$ size of largest independent set contained in A

$\mathcal{I} =$ {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

Representable: matroid that comes form a matrix *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*, with for all $A, B \subseteq E$:

  (r1) $0 \leq r(A) \leq \dim A$

  (r2) If $A \subseteq B$ then $r(A) \leq r(B)$.

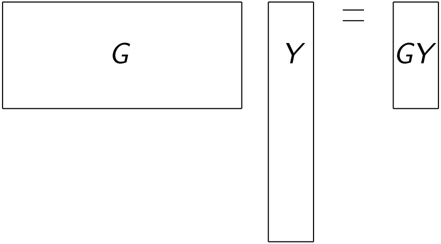
  (r3) $r(A+B) + r(A \cap B) \leq r(A) + r(B)$ (semimodular)

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* $\mathbb{F}_q$.

We call a q-matroid that comes from a code *representable*.

Conjecture (J. & Torielli, 2017)
All q-matroids are representable.

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 $\mathbb{F}_{q^m}$.

Motivating evidence:

- uniform matroids are representable;
- the matrix has entries in an extension field.

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 $\mathcal{I} = \left\{ \left\langle \begin{matrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{matrix} \right\rangle \text{ and all its subspaces} \right\}$.

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

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

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* $I + J$.

Theorem

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

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

(B1) $\mathcal{B} \neq \emptyset$

(B2) *If $B_1, B_2 \in \mathcal{B}$ and $B_1 \subseteq B_2$, then $B_1 = B_2$.*

(B3) *If $B_1, B_2 \in \mathcal{B}$, then for every codimension 1 subspace A of B_1 with $B_1 \cap B_2 \subseteq A$ there is a 1-dimensional subspace y of B_2 with $A + y \in \mathcal{B}$.*

(B4) *Let $A, B \subseteq E$ and let I, J be maximal intersections of some bases with A and B, respectively. Then there is a maximal intersection of a basis and $A + B$ that is contained in $I + J$.*

Duality

Let $r^*(A) = \dim A - r(M) + r(A^\perp)$.

Theorem
$M^* = (E, r^*)$ is a q-matroid, i.e., r^* satisfies (r1),(r2),(r3).

Lemma
$\mathcal{B}(M^*)$ are the orthogonal complements of bases of M.

Restriction

Let H a hyperplane in E and let $r_{M|_H}(A) = r_M(A)$.

Theorem
$M|_H = (H, r_{M|_H})$ *is a q-matroid, i.e.,* $r_{M|_H}$ *satisfies (r1),(r2),(r3).*

Lemma
$\mathcal{I}(M|_H)$ *are the independent spaces of* M *that are contained in* H*.*

Contraction

Let e 1-dim subspace of E,
$\pi : E \to E/e$ projection,
A in E/e and B in E such that $e \subseteq B$ and $\pi(B) = A$.

Let $r_{M/e}(A) = r_M(B) - 1$.

Theorem
$M/e = (E/e, r_{M/e})$ is a q-matroid, i.e., $r_{M/e}$ satisfies (r1),(r2),(r3).

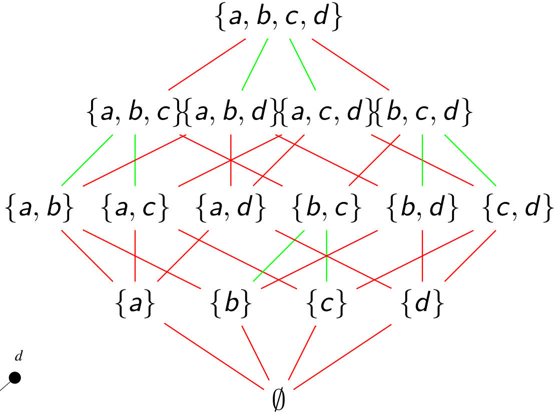
Lemma
$\mathcal{I}(M/e)$ are the independent spaces of M that contain e, projected to E/e.

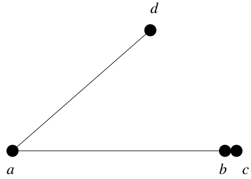
Restriction, contraction, and duality

Theorem

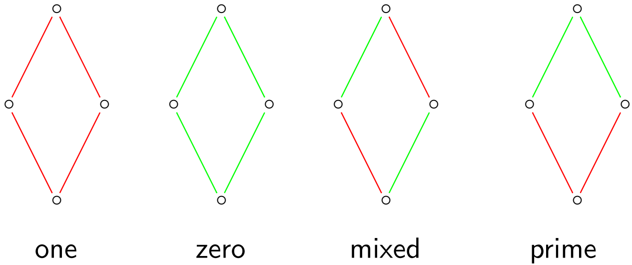
Restriction and contraction are dual operations:
$(M/e)^* = M^*|_{e^\perp}$ *and* $(M|_{e^\perp})^* = M^*/e$.

Example



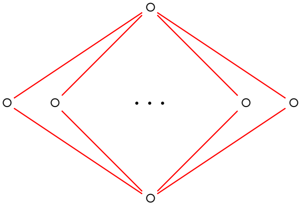


Matriod $\Longleftrightarrow$ only the following diamonds:

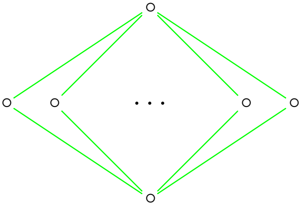


q-analogue: change Boolean lattice to subspace lattice
(or another complemented modular lattice)

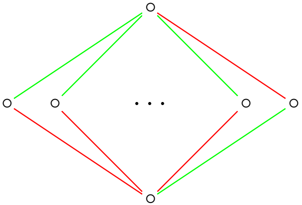
q-Matriod $\Longleftrightarrow$ only the following "diamonds":



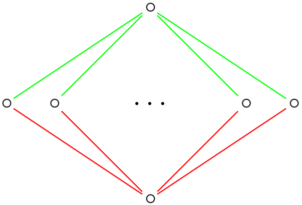
one



zero

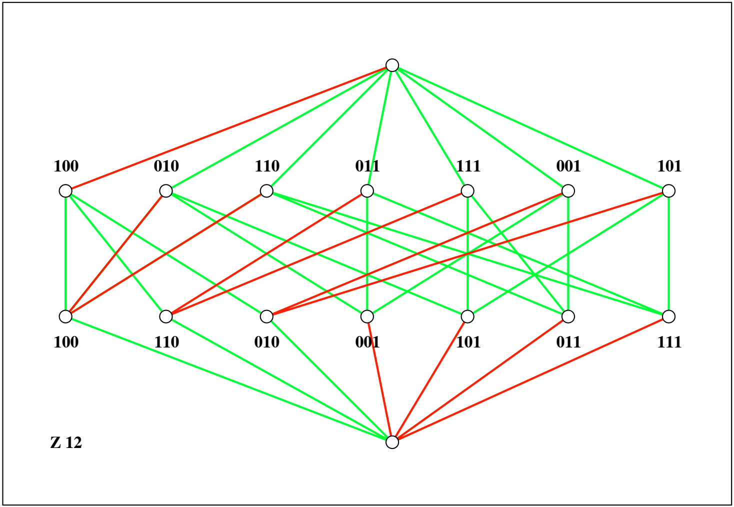


mixed

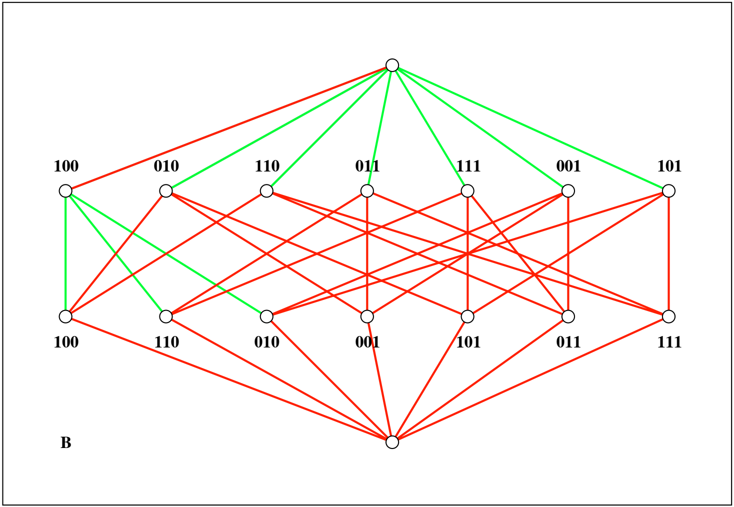


prime

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 ??

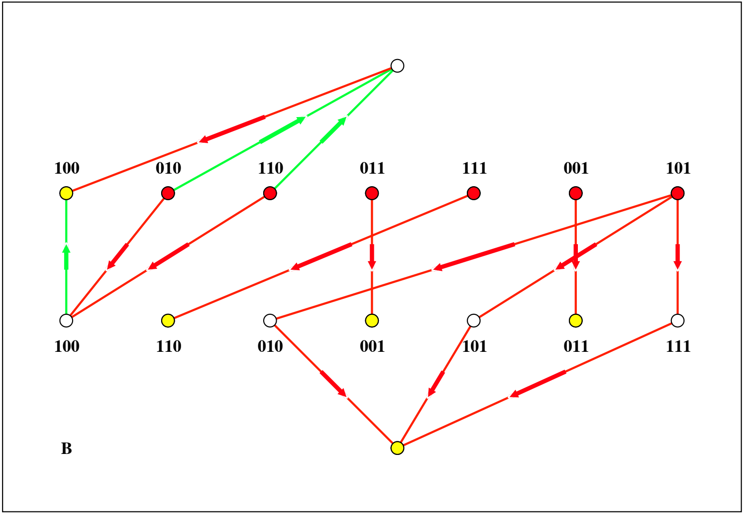
Internal/external activity induces partition of lattice in prime-free minors; that gives the Tutte polynomial.

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?