The dual q-matroid and the q-analogue of a complement

Relinde Jurrius

University of Neuchâtel, Switzerland

ALCOMA
March 20, 2015

q-Analogues

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

Example

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

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

$$= \prod_{i=0}^{k-1} \frac{q^n - q^i}{q^k - q^i}$$

Motivation: network coding

Codewords are vectors:

  ‘Ordinary’ error-correcting codes

Codewords are matrices:

  Rank metric codes

  q-analogue of ‘ordinary’ codes

Codewords are subspaces:

  Subspace codes

  Constant dimension, constant weight: q-design

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	??
difference	??

From q-analogue to 'normal': let $q \to 1$.

Matroids and q-matroids

Matroid: a pair $(E, \mathcal{B})$ with

- E finite set;
- $\mathcal{B} \subseteq 2^E$ family of subsets of E, the *bases*, with:
  - (B1) $\mathcal{B} \neq \emptyset$
  - (B2) If $B_1, B_2 \in \mathcal{B}$ then $|B_1| = |B_2|$.
  - (B3) If $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 - B_2$, then there is a $y \in B_2 - B_1$ such that $B_1 - x \cup \{y\} \in \mathcal{B}$.

Examples:

- Set of vectors; basis = maximal linearly independent subset
- Set of edges of a graph; basis = maximal cycle-free subset

q-Analogue of complement

Candidates for complement A^c of $A \subseteq E$:

- All vectors outside A

  But: not a space

q-Analogue of complement

Candidates for complement A^c of $A \subseteq E$:

- All vectors outside A

  But: not a space

- Orthogonal complement

  But: $A \cap A^{\perp}$ can be nontrivial

q-Analogue of complement

Candidates for complement A^c of $A \subseteq E$:

- All vectors outside A
  But: not a space
- Orthogonal complement
  But: $A \cap A^{\perp}$ can be nontrivial
- Quotient space E/A
  But: changes ambient space

q-Analogue of complement

Candidates for complement A^c of $A \subseteq E$:

- All vectors outside A
  But: not a space
- Orthogonal complement
  But: $A \cap A^{\perp}$ can be nontrivial
- Quotient space E/A
  But: changes ambient space
- Subspace such that $A \oplus A^c = E$
  But: not unique

q-Analogue of complement

Candidates for complement A^c of $A \subseteq E$:

- All vectors outside A
  But: not a space
- Orthogonal complement
  But: $A \cap A^\perp$ can be nontrivial
- Quotient space E/A
  But: changes ambient space
- Subspace such that $A \oplus A^c = E$
  But: not unique
- All subspaces such that $A \oplus A^c = E$
  But: more than one space

q-Analogue of complement

Solution for q-matroids:

$E - A$ is a subspace such that $(E - A) \oplus A = E$,
so $(E - A) \cap A = \mathbf{0}$.

When used, we show independence of choice of $E - A$.

$x \subseteq E - A$ independent of choice $\rightarrow x \subseteq E, x \not\subseteq A$.

Differences: $A - B$ is complement of $A \cap B$ in A.

Matroids and q-matroids

q-Matroid: a pair $(E, \mathcal{B})$ with

- E finite space;
- $\mathcal{B} \subseteq 2^E$ family of subspaces of E, the *bases*, with:
  - (B1) $\mathcal{B} \neq \emptyset$
  - (B2) If $B_1, B_2 \in \mathcal{B}$ then $\dim B_1 = \dim B_2$.
  - (B3) If $B_1, B_2 \in \mathcal{B}$ and $x \subseteq B_1$, $x \not\subseteq B_2$ a 1-dimensional subspace, then for every choice of $B_1 - x$ there is a 1-dimensional subspace $y \subseteq B_2$, $y \not\subseteq B_1$ such that $B_1 - x + y \in \mathcal{B}$.

Example: rank metric code $C \subseteq \mathbb{F}_{q^m}^n$

Why study q-matroids?

Matroids generalize:

- codes
- graphs
- some designs

q-Matroids generalize:

- rank metric codes
- q-graphs ?
- q-designs ?

Duality in matroids

$M = (E, \mathcal{B})$ a matroid, define $\mathcal{B}^* = \{E - B : B \in \mathcal{B}\}$.

Theorem
$M^* = (E, \mathcal{B}^*)$ is a matroid.

Examples:

- Matroid of dual code = dual of matroid of code
- Matroid of dual planar graph = dual of matroid of graph

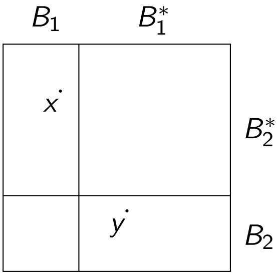
Duality in matroids

$\mathcal{B}^* = \{E - B : B \in \mathcal{B}\}$

Sketch of proof that $\mathcal{B}^*$ satisfies (B1), (B2), (B3):

(B1), (B2) clear.

(B3) If $B_1, B_2 \in \mathcal{B}$ and $x \in B_1 - B_2$, then there is a $y \in B_2 - B_1$ such that $B_1 - x \cup \{y\} \in \mathcal{B}$.



Duality in q-matroids

$M = (\mathcal{B}, E)$ a q-matroid

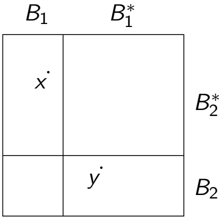
Suggestion: $\mathcal{B}^\perp = \{B^\perp : B \in \mathcal{B}\}$

Pro:

- $|\mathcal{B}^\perp| = |\mathcal{B}|$
- $M(C^\perp) = M^*(C)$ seems easy to prove

Con:

- This won't work:



Duality in q-matroids

$M = (\mathcal{B}, E)$ a q-matroid

Suggestion: $\mathcal{B}^* = \{B^* : B^* \oplus B = E \text{ for some } B \in \mathcal{B}\}$

Con:

- $|\mathcal{B}^*| =?$
- How to prove $M(C^\perp) = M^*(C)$?

Pro:

- $(E, \mathcal{B}^*)$ is a q-matroid! (Proof: straightforward q-analogue.)

Duality in q-matroids

Example

$E = \mathbb{F}_q^n$

$\mathcal{B} = \{B \subseteq E : \dim B = k\}$, $k \leq n$

$(E, \mathcal{B})$ is the *uniform q-matroid*. It has $\mathcal{B}^* = \mathcal{B}^\perp$

Also, if we would allow $E = \mathbb{R}^n$, we have $\mathcal{B}^* = \mathcal{B}^\perp$.

Duality in q-matroids

Example

$E = \mathbb{F}_q^n$

$\mathcal{B} = \{B \subseteq E : \dim B = k\}$, $k \leq n$

$(E, \mathcal{B})$ is the *uniform q-matroid*. It has $\mathcal{B}^* = \mathcal{B}^\perp$

Also, if we would allow $E = \mathbb{R}^n$, we have $\mathcal{B}^* = \mathcal{B}^\perp$.

Hopeful Hypothesis

Let $B \in \mathcal{B}$, then there is a $B' \in \mathcal{B}$ such that $B' \cap B^\perp = \mathbf{0}$.

q-Analogue of complement

Things that bother me (and should bother you, too):

- How to know which q-analogue to use?
- If some q-analogue "works", does that mean the others don't?

Your ideas and opinions are welcome!

Overview and further work

- q-Analogues are studied nowadays because of network coding.
- We should study q-matroids for the same reasons we study matroids: they generalize several discrete structures.
- Duality for q-matroids is defined...
- ...But in the right way?
- Do dual rank metric codes give dual of q-matroid?
- Duality in terms of independent sets, circuits, rank function?

- We need better intuition on the q-analogue of complements.

Thank you for your attention.