The (extended) rank weight enumerator and q-matroids

Relinde Jurrius Ruud Pellikaan

Vrije Universiteit Brussel, Belgium
Eindhoven University of Technology, The Netherlands

Conference on Random network codes and Designs over GF(q)
September 20, 2013

Field extension $\mathbb{F}_{q^m}/\mathbb{F}_q$ gives $\mathbb{F}_q$-isomorphism

$$\mathbb{F}_{q^m}^n \to \mathbb{F}_q^{m\times n}, \qquad \mathbf{x} \mapsto m(\mathbf{x}),$$

so vectors over $\mathbb{F}_{q^m}$ are mapped to $m \times n$ matrices over $\mathbb{F}_q$.

Rank metric code is subspace of $\mathbb{F}_{q^m} \leftrightarrow$ subspace of $\mathbb{F}_q^{m\times n}$.

q-Analogues

n	$\frac{q^n-1}{q-1}$
finite set	$\mathbb{F}_q^n$
subset	subspace
intersection	intersection
union	sum
complement	orthoplement
size	dimension
$\binom{n}{k}$	$\begin{bmatrix} n \\ k \end{bmatrix}_q$

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

C linear code

$\text{supp}(\mathbf{c}) =$ coordinates of $\mathbf{c}$ that are non-zero

$\text{wt}_H(\mathbf{c}) =$ 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

$\mathrm{Rsupp}(\mathbf{c}) =$ row space of $m(\mathbf{c})$

$\mathrm{wt}_R(\mathbf{c}) =$ dimension of support

Rank weight enumerator

$$W_C^R(X, Y) = \sum_{w=0}^{n} A_w^R X^{n-w} Y^w$$

with $A_w^R =$ number of words of weight w.

$D \subseteq C$ subcode

supp$(D) =$ union of supp$(\mathbf{d})$ for all $\mathbf{d} \in D$

wt$_H(D) =$ size of support

Generalized weight enumerators

For all $0 \leq r \leq \dim C$:

$$W_C^r(X, Y) = \sum_{w=0}^{n} A_w^r X^{n-w} Y^w$$

with $A_w^r =$ number of subcodes of dimension r and weight w.

(Note: consistent with definition of generalized Hamming weights)

$D \subseteq C$ subcode

$\mathrm{Rsupp}(D) =$ sum of $\mathrm{Rsupp}(\mathbf{d})$ for all $\mathbf{d} \in D$

$\mathrm{wt}_R(D) =$ dimension of support

Generalized rank weight enumerators

For all $0 \le r \le \dim C$:

$$W_C^{R,r}(X,Y) = \sum_{w=0}^{n} A_w^{R,r} X^{n-w} Y^w$$

with $A_w^{R,r}$ = number of subcodes of dimension r and weight w.

(Note: consistent with definition of generalized rank weights)

$\mathbb{F}_{q^e}/\mathbb{F}_q$ field extension

Extension code $C \otimes \mathbb{F}_{q^e}$: code over $\mathbb{F}_{q^e}$ generated by words of C.

Extended weight enumerator

$$W_C(X,Y,T) = \sum_{w=0}^{n} A_w(T) X^{n-w} Y^n$$

with $A_w(T)$ polynomial such that $A_w(q^e) =$ number of words of weight w in $C \otimes \mathbb{F}_{q^e}$.

$\mathbb{F}_{q^{me}}/\mathbb{F}_{q^m}$ field extension

Extension code $C \otimes \mathbb{F}_{q^{me}}$: code over $\mathbb{F}_{q^{me}}$ generated by words of C.

Extended rank weight enumerator

$$W_C^R(X, Y, T) = \sum_{w=0}^{n} A_w^R(T) X^{n-w} Y^n$$

with $A_w^R(T)$ polynomial such that $A_w^R(q^{me})$ = number of words of weight w in $C \otimes \mathbb{F}_{q^{me}}$.

J subset of $[n]$

$$C(J) = \{\mathbf{c} \in C : \mathrm{supp}(\mathbf{c}) \subseteq J^c\}$$

Lemma

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

$$l(J) = \dim_{\mathbb{F}_q} C(J)$$

J subspace of $\mathbb{F}_q^n$

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

Lemma

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

$$l(J) = \dim_{\mathbb{F}_{q^m}} C(J)$$

Determining extended weight enumerator

$\longleftrightarrow$

Determining generalized weight enumerators

$\longleftrightarrow$

Determining $l(J)$ for all $J \subseteq [n]$

Determining extended rank weight enumerator

$\longleftrightarrow$

Determining generalized rank weight enumerators

$\longleftrightarrow$

Determining $l(J)$ for all $J \subseteq \mathbb{F}_q^n$

Matroid

E finite subset

Independent sets $\mathcal{I} \subseteq 2^E$

- $\emptyset \in \mathcal{I}$
- If $A \in \mathcal{I}$ and $B \subseteq A$ then $B \in \mathcal{I}$.
- If $A, B \in \mathcal{I}$ and $|A| > |B|$ then there is an $a \in A \setminus B$ such that $B \cup \{a\} \in \mathcal{I}$.

Rank function $r : 2^E \to \mathbb{N}$

- $0 \leq r(A) \leq |A|$
- If $A \subseteq B$ then $r(A) \leq r(B)$.
- $r(A \cup B) + r(A \cap B) \leq r(A) + r(B)$ (semimodular)

Fact: a linear code gives a matroid with

$$E = \text{ columns of generator matrix}$$

$$r(J) = \text{ dimension of subspace spanned by vectors of } J$$

Theorem

$r(J) = \dim C - l(J)$

Rank generating function

$$R_M(X,Y) = \sum_{J\subseteq E} X^{r(E)-r(J)} Y^{|J|-r(J)}$$

(Tutte polynomial: replace X by $X-1$ and Y by $Y-1$.)

Theorem (Greene, 1976)

The Tutte polynomial determines the weight enumerator.

Theorem

The extended weight enumerator determines the Tutte polynomial and vice versa.

q-Matroid

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

q-independent sets $\mathcal{I} \subseteq \{\text{subspaces of } E\}$

- $\mathbf{0} \in \mathcal{I}$
- If $A \in \mathcal{I}$ and $B \subseteq A$ then $B \in \mathcal{I}$.
- If $A, B \in \mathcal{I}$ and $\dim A > \dim B$ then there is a 1-dimensional subspace $a \subseteq A$, $a \not\subseteq B$ such that $B + a \in \mathcal{I}$.

q-Rank function $r : \{\text{subspaces of } E\} \to \mathbb{N}$

- $0 \leq r(A) \leq \dim A$
- If $A \subseteq B$ then $r(A) \leq r(B)$.
- $r(A + B) + r(A \cap B) \leq r(A) + r(B)$ (semimodular)

Theorem

Let $r(J) = \dim C - l(J)$ *for a rank metric code* C*. Then* $r(J)$ *is the rank function of a q-matroid.*

Lemma

$$l(A + B) + l(A \cap B) \geq l(A) + l(B)$$

q-Rank generating function

$$R_M^q(X,Y) = \sum_{J \subseteq \mathbb{F}_q^n} X^{r(E)-r(J)} Y^{\dim J - r(J)}$$

Question: Are the extended rank weight enumerator and the q-rank generating function equivalent?

Answer: Not sure, but probably "yes".

Why study q-matroids?

Matroids generalize:

- codes
- graphs
- some designs

q-Matroids generalize:

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

Further work

- Equivalence between polynomials
- Various definetions of q-matroids
- “Representable” q-matroids
- Deletion and contraction

Thank you for your attention.

e element of finite set E

$$\{\text{subsets containing } e\} \cup \{\text{subsets of } e^c\} = 2^E$$

e 1-dimensional subspace of $\mathbb{F}_q^n$

$$\{\text{subspaces containing } e\} \cup \{\text{subspaces of } e^\perp\} \neq \{\text{all subspaces of } \mathbb{F}_q^n\}$$