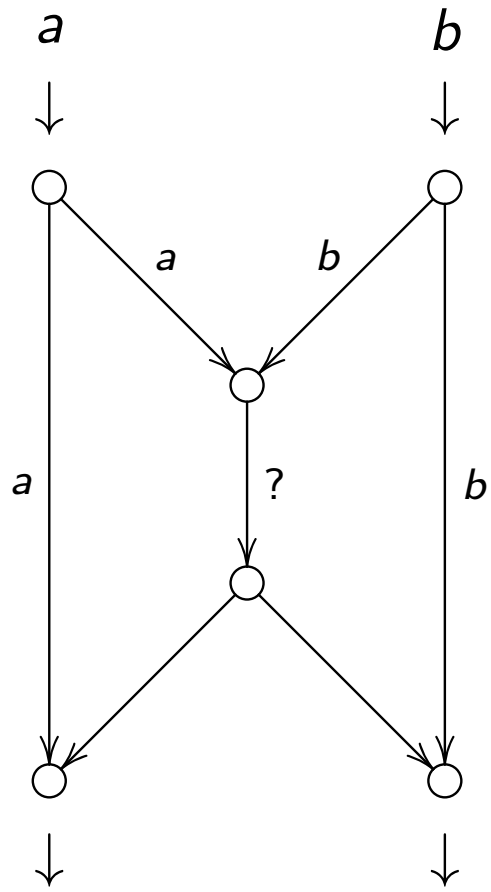
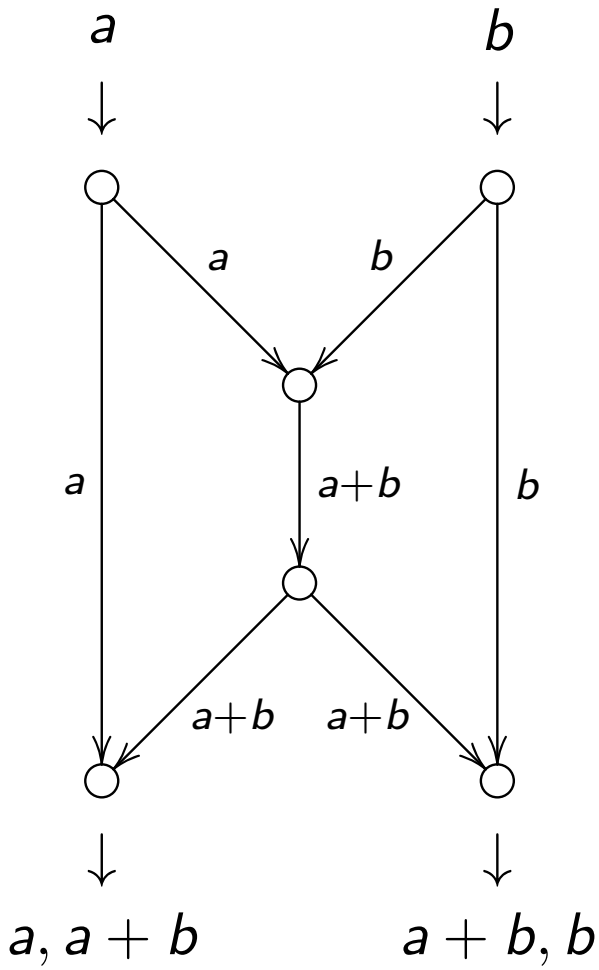
The (extended) rank weight enumerator and q-matroids

Relinde Jurrius Ruud Pellikaan

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

Academy Contact Forum "Coding Theory and Cryptography V"
October 4, 2013


a
b
a
b
a
?
b



Idea: send (rows of) matrices instead of vectors

Send: $X_1, \ldots, X_m \in \mathbb{F}_q^n$

Receive: $Y_1, \ldots, Y_m \in \mathbb{F}_q^n$

No errors: $Y = AX$

A full rank, known from the network structure

In practice: $Y = A'X + Z$

A' rank erasures

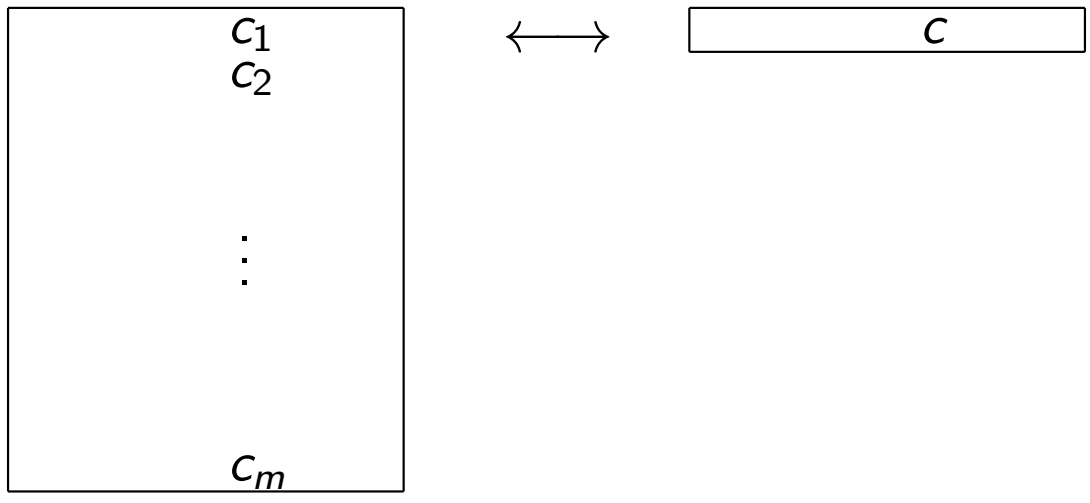
Z errors

Decoding possible if $\mathrm{rk}(A')$ not too small and $\mathrm{rk}(Z)$ not too big.

Rank metric: $d(X, Y) = \mathrm{rk}(X - Y)$

$\mathbb{F}_{q^m}/\mathbb{F}_q$ field extension with basis $\alpha_1, \ldots, \alpha_m$.

Write $c = c_1\alpha_1 + \ldots + c_m\alpha_m$.



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

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

Question: Which vectors can appear as rows of $m(\mathbf{x})$?

$\mathrm{Tr} : \mathbb{F}_{q^m} \to \mathbb{F}_q, \qquad x \mapsto x + x^q + x^{q^2} + \ldots + x^{q^{m-1}}$

$\mathrm{Frob} : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m}, \quad x \mapsto x^q$

Component-wise defined on vectors.

Trace code $\mathrm{Tr}(C)$: all vectors in the image of Tr applied to C

Galois closure C^*: smallest space containing C, closed under Frob

Galois closed: $C = C^*$

Theorem (Giorgetti, Previtali, 2010)

The following are equivalent:

- $C \subseteq \mathbb{F}_{q^m}^n$ *Galois closed*
- C *has a basis over* $\mathbb{F}_q^n$
- $C = Tr(C) \otimes \mathbb{F}_{q^m}$

Theorem

Rows of all $m(\mathbf{c})$ *with* $\mathbf{c} \in C \longleftrightarrow$ *vectors of* $Tr(C)$

Corollary

$rk(\mathbf{c}) \leq \dim(Tr(C))$

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

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

$\mathrm{wt}_H(\mathbf{c}) =$ 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 rank weight w.

J subset of $[n]$

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

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

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

$$B_J = |C(J)| - 1 = q^{l(J)} - 1$$

$$B_t = \sum_{|J|=t} B_J$$

Lemma

$$B_t = \sum_{w=0}^{n} \binom{n-w}{t} A_w$$

Determining $W_C(X, Y) \longleftrightarrow$ determining $l(J)$ for all $J \subseteq [n]$

$$B_J^R = |C(J)| = q^{m \cdot l(J)}$$

$$B_t^R = \sum_{\dim J = t} B_J^R$$

Lemma

$$B_t^R = \sum_{w=0}^{n} \begin{bmatrix} n-w \\ t \end{bmatrix}_q A_w^R$$

Determining $W_C^R(X, Y) \longleftrightarrow$ determining $l(J)$ for all $J \subseteq \mathbb{F}_q^n$

$D \subseteq C$ subcode

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

$\mathrm{wt}_H(D) =$ 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.

$D \subseteq C$ 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 $0 \leq r \leq \dim C$:

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

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

Generalized Hamming weights: smallest w such that A_w^r is nonzero. Studied by Klöve, 1978; Wei, 1991.

Lemma

The definition of the generalized weight enumerator agrees with the definition of the generalized Hamming weights.

Generalized rank weights: smallest w such that $A_w^{R,r}$ is nonzero. Studied by Oggier, Sboui, 2012; Kurihara, Matsumoto, Uyematsu, 2013; Ducoat, 2013.

Lemma

The definition of the generalized rank weight enumerator agrees with the definitions of the generalized rank weights.

Lemma

$Rsupp(D) = Tr(D)$

$\mathbb{F}_{q^e}/\mathbb{F}_q$ 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 rank weight w in $C \otimes \mathbb{F}_{q^{me}}$.

Determining extended weight enumerator

$\longleftrightarrow$

Determining generalized weight enumerators

$\longleftrightarrow$

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

Determining extended rank weight enumerator

$\longleftrightarrow$

Determining generalized rank weight enumerators

$\longleftrightarrow$

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

Matroid

E finite set

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

$E =$ index set for columns of generator matrix

$r(J) =$ 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 spaces $\mathcal{I} \subseteq \{\text{subspaces of } E\}$

- $\mathbf{0} \in \mathcal{I}$
- 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?

Naive attempt: Try to mimic formulas for normal case.

$$W_C(X, Y, T) = (X - Y)^k Y^{n-k} R_M\left(\frac{TY}{X - Y}, \frac{X - Y}{Y}\right)$$

$$R_M(X, Y) = (Y + 1)^n Y^{-k} W_C(1, (Y + 1)^{-1}, XY)$$

Almost works...

More sophisticated attempt: q-analogue of Greene's proof?

Codes: puncturing and shortening
Matroids: deletion and contraction

Theorem
The deletion/contraction of a matroid M of an element e is a matroid with ground set $E - e$ and rank function

- *Deletion:* $r_{M-e}(A) = r_M(A)$
- *Contraction:* $r_{M/e}(A) = r_M(A \cup \{e\}) - 1$

$$
\begin{aligned}
R_M(X,Y) &= \sum_{\substack{J\subseteq E\\ e\notin J}} X^{r(E)-r(J)}\,Y^{|J|-r(J)} + \sum_{\substack{J\subseteq E\\ e\in J}} X^{r(E)-r(J)}\,Y^{|J|-r(J)} \\
&= R_{M-e}(X,Y) + R_{M/e}(X,Y)
\end{aligned}
$$

Theorem (Brylawski, Oxley, 1992)

Everything that behaves nicely with deletion/contraction is related to the rank generating function.

Greene: weight enumerator behaves nicely

Theorem

The deletion/contraction of a q-matroid M of a 1-dimensional subspace e is a q-matroid with ground space $e^{\perp}$ and rank function

- *Deletion:* $r_{M-e}(A) = r_M(A)$
- *Contraction:* $r_{M/e}(A) = r_M(A + e) - 1$

e element of finite set E

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

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

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

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
- Duality of q-matroids and link with (known) MacWilliams relations for rank weight enumerator
- Various definitions of q-matroids
- "Representable" q-matroids
- Puncturing and shortening for rank metric codes
- Deletion and contraction

Thank you for your attention.