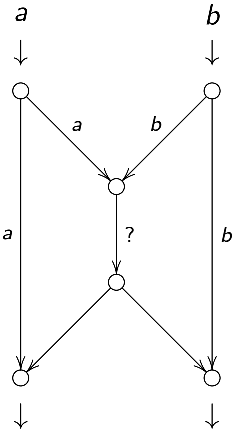
The extended and generalized rank weight enumerator

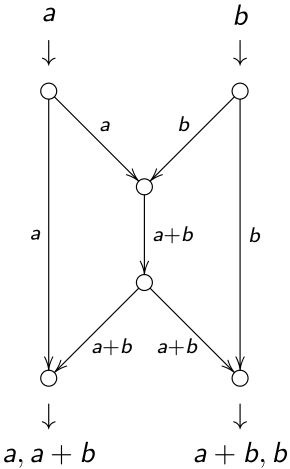
Relinde Jurrius
(joint work with Ruud Pellikaan)

University of Neuchâtel, Switzerland

Mathematics of Communications
January 27, 2015



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

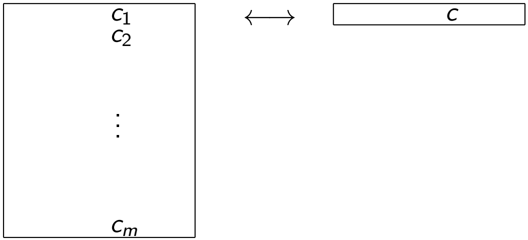
Z errors

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



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

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

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

$\text{wt}_R(\mathbf{c}) =$ 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 $[n]$

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

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

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

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

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

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

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.

$D \subseteq C$ subcode

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

$\text{wt}_R(D) =$ 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

$\mathbb{F}_{q^e}/\mathbb{F}_q$ 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 $l(J)$ for all $J \subseteq [n]$

Determining extended rank weight enumerator

$\longleftrightarrow$

Determining generalized rank weight enumerators

$\longleftrightarrow$

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

Work in progress:

generalize to codes over arbitrary fields

Linear codes are subspaces of K^n

Hamming distance is still a metric

Work in progress:

generalize to codes over arbitrary fields

Rank metric codes over cyclic field extension L/K

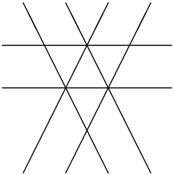
Rank distance is still a metric

(Augot, Loidreau, Robert)

Example

Hyperplane arrangement and characteristic polynomial $\chi(T)$

over $\mathbb{R}$:



$|\chi(-1)| = \#$ regions
outside arrangement

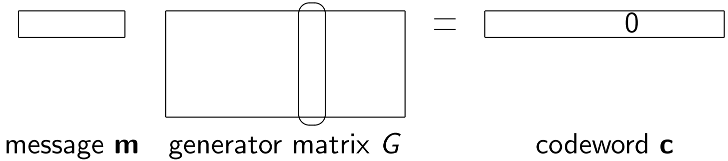
over $\mathbb{F}_q$:

?

$\chi(q) = \#$ points
outside arrangement

Complement of arrangement is a *polynomial-count variety*
$\chi(T)$ is a *counting polynomial*

Weight enumeration is like counting in hyperplane arrangement:



$c_j = 0 \iff$ **m** in hyperplane orthogonal to j-th column of G

Plesken, Bächler: Counting polynomials for linear codes $\rightsquigarrow A_w(T)$

For (extended) rank weight enumerator:

1. Find the right variety.
2. Prove it is a polynomial-count variety.
3. Find the right counting polynomial.

1 and 3 follow from before; 2 is more difficult

Thank you for your attention.

PS: We're hiring!
PhD student or postdoc in
distributed storage systems