The extended and generalized rank weight enumerator

Relinde Jurrius
(joint work with Ruud Pellikaan)

University of Neuchâtel, Switzerland

Mathematics of Communications
January 27, 2015
\( \mathbb{F}_{q^m}/\mathbb{F}_q \) field extension with basis \( \alpha_1, \ldots, \alpha_m \).

Write \( c = c_1 \alpha_1 + \ldots + c_m \alpha_m \).

\[ \begin{array}{c}
  c_1 \\
  c_2 \\
    \vdots \\
  c_m
\end{array} \quad \leftrightarrow \quad \begin{array}{c}
  \quad c
\end{array} \]

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

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

\[
\begin{align*}
\text{finite set} & \quad \frac{q^n - 1}{q - 1} \\
\text{subset} & \quad \mathbb{F}_q^n \\
\text{intersection} & \quad \text{intersection} \\
\text{union} & \quad \text{sum} \\
\text{size} & \quad \binom{n}{k} \\
\text{dimension} & \quad [n]_q \\
\end{align*}
\]

From $q$-analogue to ‘normal’: let $q \to 1$. 
A linear code

\[ \text{supp}(c) = \text{coordinates of } c \text{ that are non-zero} \]
\[ \text{wt}_H(c) = \text{size of support} \]

**Weight enumerator**

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

with \( A_w = \text{number of words of weight } w. \)
C rank metric code

$R_{\text{supp}}(c) = \text{row space of } m(c)$

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

Rank weight enumerator

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

with $A_w^R = \text{number of words of rank weight } w$. 
\[ J \text{ subset of } [n] \]

\[ C(J) = \{ c \in C : \text{supp}(c) \subseteq J^c \} \]

Lemma

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

\[ l(J) = \dim_{\mathbb{F}_q} C(J) \]
$J$ subspace of $\mathbb{F}_q^n$

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

Lemma

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

$$I(J) = \dim_{\mathbb{F}_q^m} C(J)$$
\[ B_J = |C(J)| - 1 = q^{l(J)} - 1 \]

\[ B_t = \sum_{|J|=t} B_J \]

Lemma

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

Determining \( W_C(X, Y) \) \( \Longleftrightarrow \) determining \( l(J) \) for all \( J \subseteq [n] \)
$B_J^R = |C(J)| = q^{m \cdot l(J)}$

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

Lemma

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

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

\[ \text{supp}(D) = \text{union of supp}(d) \text{ for all } d \in D \]
\[ \text{wt}_H(D) = \text{size of support} \]

Generalized weight enumerators

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

\[ W^r_C(X, Y) = \sum_{w=0}^{n} A^r_w X^{n-w} Y^w \]

with $A^r_w = \text{number of subcodes of dimension } r \text{ and weight } w$. 
$D \subseteq C$ subcode

$R_{\text{supp}}(D) = \text{sum of } R_{\text{supp}}(d) \text{ for all } d \in D$

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

**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 $A_w^{R,r} = \text{number of subcodes of dimension } r \text{ and rank weight } w$
$\mathbb{F}_{q^e}/\mathbb{F}_q$ 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 $C \otimes \mathbb{F}_{q^e}$. 
\( \mathbb{F}_{q^m}/\mathbb{F}_q \) field extension

Extension code \( C \otimes \mathbb{F}_{q^m} \): code over \( \mathbb{F}_{q^m} \) 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 \( C \otimes \mathbb{F}_{q^m} \).
Determining extended weight enumerator

$\iff$

Determining generalized weight enumerators

$\iff$

Determining $l(J)$ for all $J \subseteq [n]$
Determining extended rank weight enumerator

\[ \leftrightarrow \]

Determining generalized rank weight enumerators

\[ \leftrightarrow \]

Determining \( l(J) \) for all \( J \subseteq F_q^n \)
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 $\mathbb{R}$:

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

over $\mathbb{F}_q$:

| $\chi(q) = \# \text{ points}$ |
| $\text{outside arrangement}$ |

Complement of arrangement is a *polynomial-count variety* $\chi(T)$ is a *counting polynomial*
Weight enumeration is like counting in hyperplane arrangement:

\[
\begin{array}{ccc}
\text{message } m & \text{generator matrix } G & \text{codeword } c \\
\end{array}
\]

\[c_j = 0 \iff m \text{ in hyperplane orthogonal to } j\text{-th column of } G\]

Plesken, Bächler: Counting polynomials for linear codes
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