

# On defining the generalized rank weight

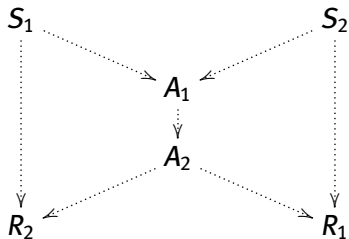
Ruud Pellikaan  
joint work with  
Relinde Jurrius

Autonomous University Barcelona, 6 November 2014

1. Introduction
2. Hamming weight
3. Rank weight
4. Extended rank weight enumerator

1. Error-correction, vectors in  $\mathbb{F}_q^n$ , Hamming weight
2. Network coding, matrices in  $\mathbb{F}_q^{m \times n}$ , rank weight
3. Wire-tap channel, generalized rank weight

Some text



$\mathbb{F}_q$  is the **finite field** with  $q$  elements

$\mathbb{F}_{q^m}$  is the **finite field extension** of  $\mathbb{F}_q$  of degree  $m$

An  $[n, k]$  **code** over  $\mathbb{F}_q$  is a subspace of  $\mathbb{F}_q^n$  of dimension  $k$

The **inner product** on  $\mathbb{F}_q^n$  is defined by

$$\mathbf{x} \cdot \mathbf{y} = x_1 y_1 + \cdots + x_n y_n$$

This inner product is bilinear, symmetric and non-degenerate

For an  $[n, k]$  code  $C$  we define the **dual** or orthogonal code  $C^\perp$  as

$$C^\perp = \{ \mathbf{x} \in \mathbb{F}_q^n \mid \mathbf{c} \cdot \mathbf{x} = 0 \text{ for all } \mathbf{c} \in C \}$$

The **support** of  $\mathbf{x}$  in  $\mathbb{F}_q^n$  is defined by

$$\text{supp}(\mathbf{x}) = \{ j \mid x_j \neq 0 \}$$

The **weight** of  $\mathbf{x}$  is defined by

$$\text{wt}(\mathbf{x}) = |\text{supp}(\mathbf{x})|$$

that is the number of nonzero entries of  $\mathbf{x}$

The support of **subspace**  $D$  of  $\mathbb{F}_q^n$  is defined by

$$\text{supp}(D) = \{ j \mid x_j \neq 0 \text{ for some } \mathbf{x} \in D \}$$

The **weight** of  $D$  is defined by

$$\text{wt}(D) = |\text{supp}(D)|$$

Let  $C$  be an  $\mathbb{F}_q$ -linear code

Then the **minimum distance** of  $C$  is

$$d(C) = \min\{ \text{wt}(c) \mid \mathbf{0} \neq c \in C \}$$

The  $r$ -th **generalized distance** of  $C$  is

$$d_r(C) = \min\{ \text{wt}(D) \mid D \text{ subspace of } C, \dim(D) = r \}$$

So  $d_1(C) = d(C)$ .

Gabidulin defined rank weight  
Applications in network coding

Choose a basis  $\alpha_1, \dots, \alpha_m$  of  $\mathbb{F}_{q^m}$  as a vector space over  $\mathbb{F}_q$

Let  $C$  be an  $\mathbb{F}_{q^m}$ -linear code of length  $n$

Let  $\mathbf{c} = (c_1, \dots, c_n)$  in  $C$

Then  $M(\mathbf{c})$  is the  $m \times n$  matrix with entries  $c_{ij}$ :

$$c_j = \sum_{i=1}^m c_{ij} \alpha_i$$



Let  $C$  be an  $\mathbb{F}_{q^m}$ -linear code of length  $n$  and  $\mathbf{c} \in C$

$\text{Rsupp}(\mathbf{c})$ , the rank support of  $\mathbf{c}$   
is by definition the **row space of  $M(\mathbf{c})$**

The **rank weight** of  $\mathbf{c}$  is

$$\text{wt}_R(\mathbf{c}) = \dim(\text{Rsupp}(\mathbf{c}))$$

The **rank distance** is defined by  $d_R(\mathbf{x}, \mathbf{y}) = \text{wt}_R(\mathbf{x} - \mathbf{y})$

This defines a **metric** on  $\mathbb{F}_{q^m}^n$

The rank distance of the code is

$$d_R(C) = \min\{ \text{wt}_R(\mathbf{c}) : \mathbf{0} \neq \mathbf{c} \in C \}$$

The  $q$ -analogue of a **finite set** is a **finite dimensional vector space**  
 We list the  $q$ -analogues of some properties of subsets:

$I, J$ subsets of $\{1, \dots, n\}$	$I, J$ subspaces of $\mathbb{F}_q^n$
$\emptyset$	$\{0\}$
$I \cap J$ intersection	$I \cap J$ intersection
$I \cup J$ union	$I + J$ sum
$ I $ , size of $I$	$\dim(I)$ , dimension of $I$
$\binom{n}{k}$ Newton binomial	$\begin{bmatrix} n \\ k \end{bmatrix}_q$ Gaussian binomial
<b>Hamming</b> distance on $\mathbb{F}_q^n$	<b>Rank</b> distance on $\mathbb{F}_{q^m}^n$
$C$ an $\mathbb{F}_q$ -linear code	$C$ an $\mathbb{F}_{q^m}$ -linear code

Let  $C$  be a linear code over  $\mathbb{F}_q$

For a subset  $J$  of  $\{1, 2, \dots, n\}$  define

$$C(J) = \{ \mathbf{c} \in C \mid c_j = 0 \text{ for all } j \in J \}$$

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

$$B_J(T) = T^{l(J)} - 1$$

$$B_t(T) = \sum_{|J|=t} B_J(T)$$

Note that  $B_J(q^m)$  is the number of nonzero codewords in  $(C \otimes \mathbb{F}_{q^m})(J)$

Then

$$W_C(X, Y, T) = X^n + \sum_{t=0}^n B_t(T)(X - Y)^t Y^{n-t}$$

This translation is sometimes **ambiguous**:

$I, J$ subsets of $\{1, \dots, n\}$ $C$ an $\mathbb{F}_q$ -linear code	$I, J$ subspaces of $\mathbb{F}_q^n$ $C$ an $\mathbb{F}_{q^m}$ -linear code
$I \cap J = \emptyset$ $J^c$ complement of $J$ $I \subseteq J^c$ $C(J) = \{\mathbf{c} \in C : c_j = 0, \forall j \in J\}$ $C(J) = \{\mathbf{c} \in C : \text{supp}(\mathbf{c}) \cap J = \emptyset\}$ $C(J) = \{\mathbf{c} \in C : \text{supp}(\mathbf{c}) \subseteq J^c\}$	$I \cap J = \{0\}$ $J^\perp$ orthoplement of $J$ $I \subseteq J^\perp$ ??? $C(J) = \{\mathbf{c} \in C : \text{Rsupp}(\mathbf{c}) \cap J = \{0\}\}$ $C(J) = \{\mathbf{c} \in C : \text{Rsupp}(\mathbf{c}) \subseteq J^\perp\}$

Let  $C$  be an  $\mathbb{F}_{q^m}$ -linear code of length  $n$

For an  $\mathbb{F}_q$ -linear subspace  $J$  of  $\mathbb{F}_q^n$  define

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

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

$$B_J^R(T) = T^{m \cdot l(J)}$$

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

Then

$B_J^R(q)$  is the number of codewords in  $C(J)$

The extended rank weight enumerator is given by

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

Now

$A_j^R(q)$  is the number of codewords in  $C$  of rank weight  $w$

and

$$A_w^R(T) = \sum_{t=n-w}^n (-1)^{t-n+w} T^{\binom{t-n+w}{2}} \begin{bmatrix} t \\ n-w \end{bmatrix}_T B_t^R(T)$$

**THANKS!**

**QUESTIONS?**