The extended and generalized rank weight enumerator of a code

Ruud Pellikaan
joint work with
Relinde Jurrius

ACA-2014, CACTC, New York, 9 July 2014

Content

1. Hamming weight
2. Extended and generalized weight enumerator
3. Rank weight
4. Extended rank weight enumerator

Notation

$\mathbb{F}_q$ 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

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

Support and weight

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

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

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

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

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

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

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

The weight of D is defined by

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

Generalized Hamming weight

Let C be an $\mathbb{F}_q$-linear code
Then the minimum distance of C is

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

The r-th generalized distance of C is

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

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

(Generalized) weight enumerator

Let C be a code of length n
A_w denotes the number of codewords in C of weight w
$A_w^{(r)}$ denotes the number of subspaces of C of dimension r weight w

The weight enumerator is:

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

The r-th generalized weight enumerator is:

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

Extended code

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

Consider the code $C \otimes \mathbb{F}_{q^m}$ over $\mathbb{F}_{q^m}$
by taking all $\mathbb{F}_{q^m}$-linear combinations of the codewords in C
This is called the extended code of C over $\mathbb{F}_{q^m}$

Weight enumerator of extended code

Let C be a linear $[n, k]$ code over $\mathbb{F}_q$
Then there exist polynomials $A_w(T)$
with integer coefficients in the variable T
such that

$$A_w(q^m) = \text{number of codewords of weight } w \text{ in } C \otimes \mathbb{F}_{q^m}$$

Let

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

Then

$$W_C(X, Y, q^m) = W_{C \otimes \mathbb{F}_{q^m}}(X, Y)$$

Network coding

Gabidulin defined rank weight
Applications in network coding

Choose a basis $\alpha_1, \ldots \alpha_m$ 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 $\mathbf{c} = (c_1, \ldots, c_n)$ in C
Then $M(\mathbf{c})$ is the $m \times n$ matrix with entries c_{ij}:

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

Rank support, weight and distance

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

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

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

The rank distance is defined by $d_R(\mathbf{x}, \mathbf{y}) = \mathrm{wt}_R(\mathbf{x} - \mathbf{y})$
This defines a metric on $\mathbb{F}_{q^m}^n$

The rank distance of the code is

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

Dictionary

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 $\{1, \ldots, n\}$	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
$\lvert I \rvert$, size of I	$\dim(I)$, dimension of I
$\binom{n}{k}$ Newton binomial	$\begin{bmatrix} n \\ k \end{bmatrix}_q$ Gaussian binomial
Hamming distance on $\mathbb{F}_q^n$	Rank distance on $\mathbb{F}_{q^m}^n$
C an $\mathbb{F}_q$-linear code	C an $\mathbb{F}_{q^m}$-linear code

Formalism for extended weight enumerator

Let C be a linear code over $\mathbb{F}_q$
For a subset J of $\{1, 2, \ldots, n\}$ define

$$\begin{aligned} C(J) &= \{\, \mathbf{c} \in C \mid c_j = 0 \text{ for all } j \in J \,\} \\ l(J) &= \dim C(J) \\ B_J(T) &= T^{l(J)} - 1 \\ B_t(T) &= \sum_{|J|=t} B_J(T) \end{aligned}$$

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

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

Ambiguous translation of C(J)

This translation is sometimes ambiguous:

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

Extended rank weight enumerator - 1

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

$$\begin{aligned} C(J) &= \{\, \mathbf{c} \in C \;:\; \mathrm{Rsupp}(\mathbf{c}) \subseteq J^{\perp} \,\} \\ l(J) &= \dim C(J) \\ B_J^R(T) &= T^{m \cdot l(J)} \\ B_t^R(T) &= \sum_{\dim(J)=t} B_J(T) \end{aligned}$$

Then

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

Extended rank weight enumerator - 2

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?