On defining the generalized rank weight

Ruud Pellikaan
joint work with
Relinde Jurrius

Computational Aspects and Mathematical Methods for Finite Fields
and their Applications in Information Theory
ACA 2015 Kalamata, 23 July 2015

Content

Introduction

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

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

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

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 Hamming weight of D is defined by

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

Generalized Hamming weight

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

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

The r-th generalized Hamming weight of C is

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

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

Network coding

Delsarte defined rank weight
Gabidulin applied to (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 weight and distance

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

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

$$\mathrm{wt}_R(\mathbf{c}) = \mathrm{rk}(M(\mathbf{c}))$$

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

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

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
Hamming distance on $\mathbb{F}_q^n$	Rank distance on $\mathbb{F}_{q^m}^n$
Hamming weight on $\mathbb{F}_q^n$	Rank weight on $\mathbb{F}_{q^m}^n$
$\mathrm{supp}(\mathbf{c}))$	$\mathrm{Rsupp}(\mathbf{c})) =?$
$\mathrm{wt}_H(\mathbf{c})) = \lvert\mathrm{supp}(\mathbf{c})\rvert$	$\mathrm{wt}_R(\mathbf{c})) = \dim(\mathrm{Rsupp}(\mathbf{c}))$
C an $\mathbb{F}_q$-linear code	C an $\mathbb{F}_{q^m}$-linear code

Rank support

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

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

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

Let D be an $\mathbb{F}_{q^m}$-linear subcode of C
$\mathrm{Rsupp}(D)$, the rank support of D is
the $\mathbb{F}_q$-linear space generated by the $\mathrm{Rsupp}(\mathbf{d})$ with $\mathbf{d} \in D$
The rank support weight of D is

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

Galois closure

The Frobenius map

$$\varphi : \mathbb{F}_{q^m} \to \mathbb{F}_{q^m} \text{ with } \varphi(x) = x^q$$

is a field isomorphism that fixes $\mathbb{F}_q$
The extension $\mathbb{F}_{q^m}/\mathbb{F}_q$ is Galois with
cyclic Galois group generated by φ
Extend $\varphi : \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m}^n$ component-wise

Let C be an $\mathbb{F}_{q^m}$-linear subspace of $\mathbb{F}_{q^m}^n$
C^* is the Galois closure of C it is the smallest subspace of $\mathbb{F}_{q^m}^n$
that contains C and that is closed under the action of φ

A subspace is called Galois closed if and only if it is equal to its own Galois closure

Restriction – extension

Let $C \subseteq \mathbb{F}_{q^m}^n$ be an $\mathbb{F}_{q^m}$-linear subspace
The restriction of C is defined by

$$C|\mathbb{F}_q = C \cap \mathbb{F}_q^n$$

Let $D \subseteq \mathbb{F}_q^n$ be an $\mathbb{F}_q$-linear subspace
$D \otimes \mathbb{F}_{q^m}$ is the extension of D
it is the $\mathbb{F}_{q^m}$-linear subspace of $\mathbb{F}_{q^m}^n$ generated by D

Trace

The trace map

$$\mathrm{Tr} : \mathbb{F}_{q^m} \to \mathbb{F}_q$$

is defined by

$$x \mapsto x^q + \cdots + x^{q^m}$$

Extend $\mathrm{Tr} : \mathbb{F}_{q^m}^n \to \mathbb{F}_q^n$ component-wise

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

$$\mathrm{Tr}(C) = \{ \mathrm{Tr}(\mathbf{c}) \mid \mathbf{c} \in C \}$$

Summary

$$\begin{array}{ccc} C & \hookrightarrow & C^* \\ \uparrow & \searrow & \uparrow \otimes \mathbb{F}_{q^m} \\ C|\mathbb{F}_q & \hookrightarrow & \mathrm{Tr}(C) \end{array}$$

Theorem (Giorgetti-Previtali 2010)

Let C be an $\mathbb{F}_{q^m}$-linear code
Then the following statements are equivalent:

- C is Galois closed: $C = C^*$
- C is the extension of its restriction: $C = (C|\mathbb{F}_q) \otimes \mathbb{F}_{q^m}$
- C has a basis in $\mathbb{F}_q^n$.
- The trace of C is equal to its restriction: $\mathrm{Tr}(C) = C|\mathbb{F}_q$

Rsupp is Trace

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

Then the rows of the matrix $M(\mathbf{c})$ are
elements of the trace code $\mathrm{Tr}(C)$

Furthermore

$$\mathrm{Rsupp}(C) = \mathrm{Tr}(C)$$

Corollary

Let D be a subcode of the $\mathbb{F}_{q^m}$-linear code C
Then

$$\mathrm{Rsupp}(D) = \mathrm{Tr}(D)$$

and therefore

$$d_{R,r}(C) = \min_{\substack{D \subseteq C \\ \dim(D)=r}} \mathrm{wt}_R(D) = \min_{\substack{D \subseteq C \\ \dim(D)=r}} \dim \mathrm{Tr}(C) = \min_{\substack{D \subseteq C \\ \dim(D)=r}} \dim D^*$$

Generalized rank weight

Several definitions are proposed for the generalized rank weight:

1. 2012 Oggier-Sboui
2. 2012 Kurihara-Matsumoto-Uyematsu
3. 2013 Ducoat
4. 2014 Jurrius-Pellikaan
5. 2015 Martínez-Peñas

Definition Oggier-Sboui

C an $\mathbb{F}_{q^m}$-linear code

The r-th generalized rank weight of C

is defined by Oggier-Sboui as

$$\min_{\substack{D \subseteq C \\ \dim(D)=r}} \max_{\mathbf{d} \in D} \mathrm{wt}_R(\mathbf{d})$$

– "On the existence of generalized rank weights"
IEEE Int. Symposium on Information Theory, pp. 406–410, 2012

Definition Ducoat

C an $\mathbb{F}_{q^m}$-linear code

The r-th generalized rank weight of C

is defined by Ducoat as

$$\min_{\substack{D \subseteq C \\ \dim(D)=r}} \max_{\mathbf{d} \in D^*} \mathrm{wt}_R(\mathbf{d})$$

– “Generalized rank weights: a duality statement”
Contemporary Mathematics, vol. 632, pp. 101–109, 2015

Definition Kurihara-Matsumoto-Uyematsu

C an $\mathbb{F}_{q^m}$-linear code

The r-th generalized rank weight of C

is defined by Kurihara-Matsumoto-Uyematsu as

$$\min_{\substack{V \subseteq L^n, V = V^* \\ \dim(C \cap V) \geq r}} \dim V$$

– "New parameters of linear codes expressing security performance of universal secure network coding", Communication, Control, and Computing, 50th Annual Allerton Conference, pp. 533–540, 2012
– "Relative generalized rank weight of linear codes and its applications to network coding", arXiv:1301.5482v1, 2013

Definition Jurrius-Pellikaan

C an $\mathbb{F}_{q^m}$-linear code

The *r*-th generalized rank weight of C

$$d_{R,r}(C) = \min_{\substack{D \subseteq C \\ \dim(D)=r}} \mathrm{wt}_R(D)$$

–"On defining generalized rank weights"
arXiv:1506.02865

Definition Martínez-Peñas

Let $B = \{\mathbf{b}_1, \ldots, \mathbf{b}_n\} \subseteq \mathbb{F}_q^n$ be a basis of $\mathbb{F}_{q^m}^n$
Let $\varphi_B : \mathbb{F}_{q^m}^n \to \mathbb{F}_{q^m}^n$ be defined by
$\varphi_B(\mathbf{c}) = \mathbf{x}$ where $\mathbf{c} = \sum_i x_i \mathbf{b}_i$

Let D be an $\mathbb{F}_{q^m}$-linear code

$$\mathrm{wt}_R(D) = \min\{\, wt_H(\varphi_B(D)) \mid B \subseteq \mathbb{F}_q^n \text{ a basis of } \mathbb{F}_{q^m}^n \}$$

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

$$d_{R,r}(C) = \min_{\substack{D \subseteq C \\ \dim(D)=r}} \min\{\, wt_H(\varphi_B(D)) \mid B \subseteq \mathbb{F}_q^n \text{ a basis of } \mathbb{F}_{q^m}^n \}$$

– “On the similarities between generalized rank and Hamming weights and their applications to network coding”
arXiv:1506.04036

Conclusion

1. Oggier-Sboui
2. Ducoat
3. Kurihara-Matsumoto-Uyematsu
4. Jurrius-Pellikaan
5. Martínez-Peñas

If $m \geq n$ then,
these definitions of the generalized rank weight are equivalent

THANKS!

QUESTIONS?