

Generalized rank weights

Relinde Jurrius
(joint work with Ruud Pellikaan)

Vrije Universiteit Brussel, Belgium

Algebra, Codes and Networks
June 17, 2014

Generalized Hamming weights

C linear code

$\text{supp}(\mathbf{c})$ support: nonzero coordinates of word \mathbf{c}

$\text{wt}_H(\mathbf{c})$ weight: size of support of \mathbf{c}

d minimum weight of C

D subcode of C

$\text{supp}(D)$ union of supports of all $\mathbf{d} \in D$

$\text{wt}_H(D)$ size of support of D

d_r generalized Hamming weight: minimum weight of subcode of dim r

Generalized Hamming weights

Important properties

Monotonicity: $d_0 < d_1 < \dots < d_k$

Duality: $\{d_i : i \in [k]\} \dot{\cup} \{d_i^\perp : i \in [n - k]\} = [n]$

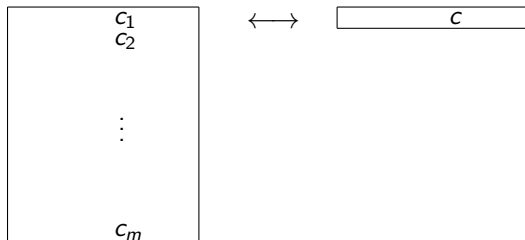
Kløve, 1978: definition, monotonicity

Wei, 1991: re-discovery, application to wiretap channels, monotonicity and duality, name

Rank metric codes

$\mathbb{F}_{q^m}/\mathbb{F}_q$ field extension with basis $\alpha_1, \dots, \alpha_m$.

Write $c = c_1\alpha_1 + \dots + c_m\alpha_m$.



$$m(\mathbf{x}) \in \mathbb{F}_q^{m \times n}$$

$$\mathbf{x} \in \mathbb{F}_{q^m}$$

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

Generalized rank weights

C linear rank metric code

$\text{Rsupp}(\mathbf{c})$ rank support: space spanned by rows of $m(\mathbf{c})$

$\text{wt}_R(\mathbf{c})$ rank weight: dimension of support of \mathbf{c} , i.e., $\text{rk}(m(\mathbf{c}))$

d minimum weight of C

D subcode of C

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

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

d_r generalized rank weight: minimum rank weight of subcode of $\dim r$

Generalized rank weights

Oggier, Sboui (2012)

$$\min_{\substack{D \subseteq C \\ \dim \bar{D} = r}} \max_{\mathbf{d} \in D} \text{rk}(m(\mathbf{d}))$$

Kurihara, Matsumoto, Uyematsu (2013)

$$\min_{\substack{V \in \mathbb{F}_q^n, V = V^* \\ \dim(C \cap V) \geq r}} \dim V$$

J, Pellikaan (2014)

$$\min_{\substack{D \subseteq C \\ \dim \bar{D} = r}} \text{wt}_R(D)$$

Generalized rank weights

OS: definition, application to rank metric wiretap channels

KMU, independently: definition, application to rank metric wiretap channels, monotonicity

Ducoat, 2014: duality,

$$\min_{\substack{V \in \mathbb{F}_{q^m}^n, V=V^* \\ \dim(C \cap V) \geq r}} \dim V = \min_{\substack{D \subseteq C \\ \dim D = r}} \max_{\mathbf{d} \in D^*} \text{rk}(m(\mathbf{d}))$$

This talk: all three definitions are equivalent

Galois closure and trace

$$\text{Tr} : \mathbb{F}_{q^m} \rightarrow \mathbb{F}_q, \quad x \mapsto x + x^q + x^{q^2} + \dots + x^{q^{m-1}}$$

$$\text{Frob} : \mathbb{F}_{q^m} \rightarrow \mathbb{F}_{q^m}, \quad x \mapsto x^q$$

Component-wise defined on vectors.

Trace code $\text{Tr}(C)$: all vectors in the image of Tr applied to C

Galois closure C^* : smallest space containing C , closed under Frob

Galois closed: $C = C^*$

Subfield subcode $C|_{\mathbb{F}_q}$: codewords with coefficients in \mathbb{F}_q

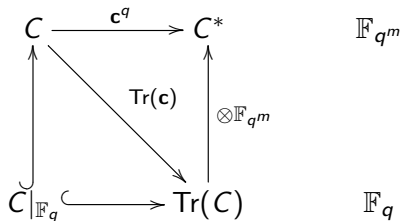
$C \subseteq \mathbb{F}_q^n$, then $C \otimes \mathbb{F}_{q^m}$: all \mathbb{F}_{q^m} -linear combinations of words of C

Galois closure and trace

Theorem (Giorgetti, Previtoli, 2010)

Let $C \subseteq \mathbb{F}_{q^m}^n$. The following are equivalent:

- ▶ C is Galois closed
- ▶ C has a basis over \mathbb{F}_q^n
- ▶ $C = \text{Tr}(C) \otimes \mathbb{F}_{q^m}$
- ▶ $\text{Tr}(C) = C|_{\mathbb{F}_q}$



Galois closure and trace

Theorem

Rows of all $m(\mathbf{c})$ with $\mathbf{c} \in C \longleftrightarrow$ vectors of $Tr(C)$

Corollary

$$rk(\mathbf{c}) \leq \dim(Tr(C))$$

Corollary

$$Rsupp(D) = Tr(D)$$

Generalized rank weights

Oggier, Sboui (2012)

$$\min_{\substack{D \subseteq C \\ \dim \bar{D} = r}} \max_{\mathbf{d} \in D} \text{rk}(m(\mathbf{d}))$$

Kurihara, Matsumoto, Uyematsu (2013)

$$\min_{\substack{V \in \mathbb{F}_q^n, V = V^* \\ \dim(C \cap V) \geq r}} \dim V$$

J, Pellikaan (2014)

$$\min_{\substack{D \subseteq C \\ \dim \bar{D} = r}} \text{wt}_R(D)$$

Theorem

For any $\mathbf{x} \in \mathbb{F}_{q^m}^n$ we have $\langle \mathbf{x} \rangle^* = \text{Rsupp}(\mathbf{x}) \otimes \mathbb{F}_{q^m}$.

Proof.

$$\langle \mathbf{x} \rangle^* \subseteq \text{Rsupp}(\mathbf{x}) \otimes \mathbb{F}_{q^m}$$

- ▶ $\langle \mathbf{x} \rangle^* = \langle \mathbf{x}, \mathbf{x}^q, \dots, \mathbf{x}^{q^{m-1}} \rangle$
- ▶ Let $(\alpha_1, \dots, \alpha_m)$ basis of \mathbb{F}_{q^m} and \mathbf{x}_i rows of $m(\mathbf{x})$
- ▶ $\mathbf{x}^{q^i} = (\alpha_1 \mathbf{x}_1 + \dots + \alpha_m \mathbf{x}_m)^{q^i} = \alpha_1^{q^i} \mathbf{x}_1 + \dots + \alpha_m^{q^i} \mathbf{x}_m$

$$\langle \mathbf{x} \rangle^* \supseteq \text{Rsupp}(\mathbf{x}) \otimes \mathbb{F}_{q^m}$$

- ▶ Rewrite $m(\mathbf{x})$ in rref with first l columns independent
- ▶ $\mathbf{x}^{q^i} = \alpha_1^{q^i} \mathbf{x}_1 + \dots + \alpha_l^{q^i} \mathbf{x}_l$ for all $i = 0, \dots, l-1$
- ▶ Vandermonde-matrix with entries $\alpha_j^{q^i}$ is invertible
- ▶ $\mathbf{x}_j \in \langle \mathbf{x}, \mathbf{x}^q, \dots, \mathbf{x}^{q^{l-1}} \rangle \subseteq \langle \mathbf{x} \rangle^*$



Theorem

For any $\mathbf{x} \in \mathbb{F}_{q^m}^n$ we have $\langle \mathbf{x} \rangle^* = R\text{supp}(\mathbf{x}) \otimes \mathbb{F}_{q^m}$.

Lemma

$$\dim \langle \mathbf{x} \rangle^* = rk(m(\mathbf{x}))$$

Lemma

For all Galois closed V there is an $\mathbf{x} \in V$ such that $V = \langle \mathbf{x} \rangle^*$.

Proof.

Pick basis of V over \mathbb{F}_q and let these vectors be rows of $m(\mathbf{x})$. \square

Theorem

$$\max_{\mathbf{d} \in D^*} \text{rk}(m(\mathbf{d})) = \dim D^* = \text{wt}_R(D)$$

Proof.

- ▶ For all $\mathbf{d} \in D^*$, $\text{Rsupp}(\mathbf{d}) \subseteq \text{Tr}(D)$ so $\text{rk}(m(\mathbf{d})) \leq \dim D^*$
- ▶ There is an $\mathbf{x} \in D^*$ such that $D^* = \langle \mathbf{x} \rangle^*$
- ▶ $\text{rk}(m(\mathbf{x})) = \dim \langle \mathbf{x} \rangle^* = \dim D^*$
- ▶ $\text{Rsupp}(D) = \text{Tr}(D)$ so $\text{wt}_R(D) = \dim \text{Tr}(D) = \dim D^*$



Generalized rank weights

Oggier, Sboui (2012)

$$\min_{\substack{D \subseteq C \\ \dim \bar{D} = r}} \max_{\mathbf{d} \in D^*} \text{rk}(m(\mathbf{d}))$$

Kurihara, Matsumoto, Uyematsu (2013)

$$\min_{\substack{V \in \mathbb{F}_q^n, V = V^* \\ \dim(C \cap V) \geq r}} \dim V$$

J, Pellikaan (2014)

$$\min_{\substack{D \subseteq C \\ \dim \bar{D} = r}} \text{wt}_R(D)$$

Theorem

$$\max_{\mathbf{d} \in D} \text{rk}(m(\mathbf{d})) = \max_{\mathbf{d} \in D^*} \text{rk}(m(\mathbf{d}))$$

Proof.

- ▶ Let $\mathbf{d} \in D^*$ with $\text{rk}(m(\mathbf{d}))$ maximal
- ▶ D^* is Galois closed, so there is an i such that $\mathbf{d}^{q^i} \in D$
- ▶ $\text{rk}(m(\mathbf{d})) = \dim \langle \mathbf{d} \rangle^*$ and $\langle \mathbf{d} \rangle^* = \langle \mathbf{d}^{q^i} \rangle^*$, so
 $\text{rk}(m(\mathbf{d})) = \text{rk}(m(\mathbf{d}^{q^i}))$



Generalized rank weights

Oggier, Sboui (2012)

$$\min_{\substack{D \subseteq C \\ \dim \bar{D} = r}} \max_{\mathbf{d} \in D^*} \text{rk}(m(\mathbf{d}))$$

Kurihara, Matsumoto, Uyematsu (2013)

$$\min_{\substack{V \in \mathbb{F}_q^n \\ \dim(C \cap V) \geq r}} \dim V$$

J, Pellikaan (2014)

$$\min_{\substack{D \subseteq C \\ \dim \bar{D} = r}} \text{wt}_R(D)$$

Theorem

$$\min_{\substack{V \subseteq \mathbb{F}_{q^m}^n, V=V^* \\ \dim(C \cap V) \geq r}} \dim V = \min_{\substack{D \subseteq C \\ \dim D=r}} \max_{\mathbf{d} \in D^*} rk(m(\mathbf{d}))$$

Proof.

- ▶ Let $V \subseteq \mathbb{F}_{q^m}^n$ such that $V = V^*$ and $\dim(C \cap V) \geq r$
- ▶ Let $D \subseteq C \cap V$ with $\dim D = r$
- ▶ Since $D \subseteq V = V^*$, we have $D^* \subseteq V^*$ so $\dim(C \cap D^*) \geq r$
- ▶ Also, for all $D \subseteq C$ with $\dim D = r$, we have that $\dim(C \cap D^*) \geq r$, so

$$\min_{\substack{V \in \Gamma(\mathbb{F}_{q^m}^n) \\ \dim(C \cap V) \geq r}} \dim V = \min_{\substack{D \subseteq C \\ \dim D=r}} \dim D^*$$

□

Summary

- ▶ Generalized rank weights are the rank metric equivalence of generalized Hamming weights.
- ▶ The three proposed definitions of the generalized rank weights are equivalent.
- ▶ When talking about Galois closure, one should also consider the trace function.

Thank you for your attention.