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

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

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

d minimum weight of C

D subcode of C

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

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

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

Generalized Hamming weights

Important properties

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

Duality: $\{d_i : i \in [k]\} \dot{\cup} \{n + 1 - d_i^{\perp} : i \in [n - k]\} = [n]$

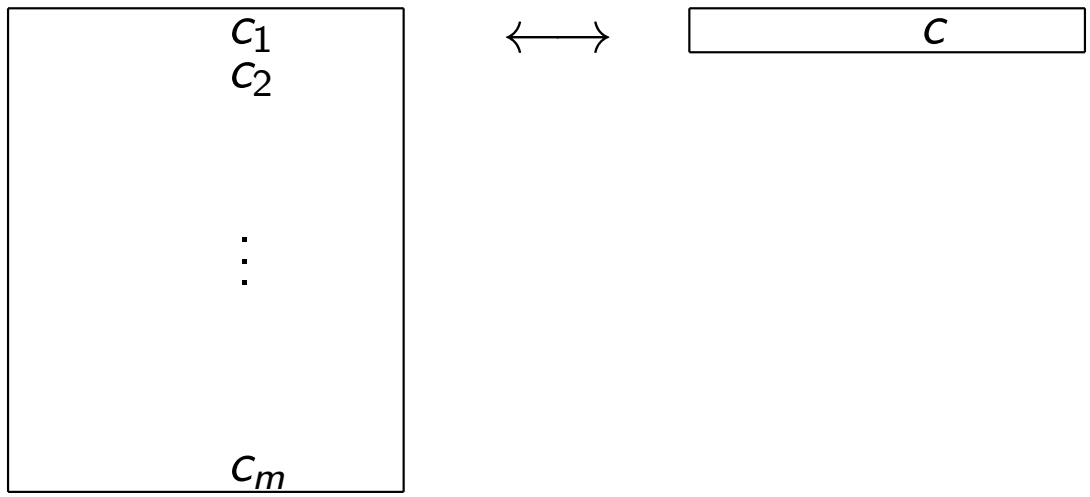
Kløve, 1978: definition, monotonicity

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 $\alpha_1, \ldots, \alpha_m$.

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



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

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

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

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

d minimum weight of C

D subcode of C

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

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

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

Generalized rank weights

Oggier, Sboui (2012)

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

Kurihara, Matsumoto, Uyematsu (2013)

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

J, Pellikaan (2014)

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

Generalized rank weights

OS: definition, application to rank metric wiretap channels

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

Ducoat, 2014: duality,

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

This talk: all three definitions are equivalent

Galois closure and trace

$\mathrm{Tr} : \mathbb{F}_{q^m} \to \mathbb{F}_q, \qquad x \mapsto x + x^q + x^{q^2} + \cdots + x^{q^{m-1}}$

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

Component-wise defined on vectors.

$C \subseteq \mathbb{F}_{q^m}^n$

Trace code $\mathrm{Tr}(C)$: 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 $\mathbb{F}_q$

$C \subseteq \mathbb{F}_q^n$

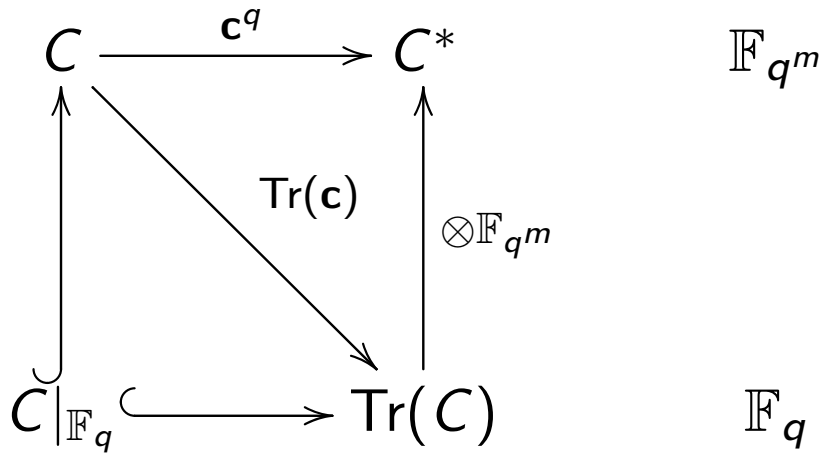
Extension code $C \otimes \mathbb{F}_{q^m}$: all $\mathbb{F}_{q^m}$-linear combinations of words of C

Galois closure and trace

Theorem (Giorgetti, Previtali, 2010)

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

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



Galois closure and trace

Theorem

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

Corollary

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

Corollary

$Rsupp(D) = Tr(D)$

Generalized rank weights

Oggier, Sboui (2012)

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

Kurihara, Matsumoto, Uyematsu (2013)

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

J, Pellikaan (2014)

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

Theorem

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

Proof.

Show the two inclusions $\langle \mathbf{x} \rangle^* \subseteq \mathrm{Rsupp}(\mathbf{x}) \otimes \mathbb{F}_{q^m}$ and $\langle \mathbf{x} \rangle^* \supseteq \mathrm{Rsupp}(\mathbf{x}) \otimes \mathbb{F}_{q^m}$. □

Lemma

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

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 $m(\mathbf{x})$. □

Theorem

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

Proof.

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

□

Generalized rank weights

Oggier, Sboui (2012)

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

Kurihara, Matsumoto, Uyematsu (2013)

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

J, Pellikaan (2014)

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

Theorem

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

Proof.

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

□

Generalized rank weights

Oggier, Sboui (2012)

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

Kurihara, Matsumoto, Uyematsu (2013)

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

J, Pellikaan (2014)

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

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.