On defining generalized rank weights

Relinde Jurrius
(joint work with Ruud Pellikaan)

Université de Neuchâtel, Switzerland

Coding & Crypto seminar
October 28, 2015

Generalized Hamming weights

C linear code

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

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

d minimum weight of C

D subcode of C

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

wt$_H$(D) size of support of D

$d_{H,r}$ generalized Hamming weight: minimum weight of subcode of dim r

Generalized Hamming weights

Important properties

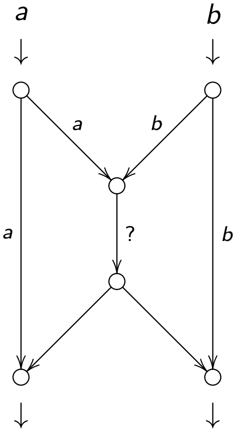
Monotonicity: $d_1 < d_2 < \cdots < d_k$

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

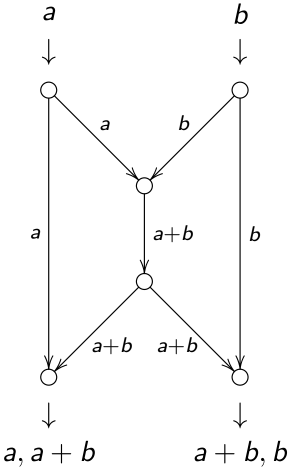
Kløve, 1978: definition, monotonicity

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

Network coding



Network coding



Idea: send (rows of) matrices instead of vectors

Send: $X_1, \ldots, X_m \in \mathbb{F}_q^n$

Receive: $Y_1, \ldots, Y_m \in \mathbb{F}_q^n$

No errors: $Y = AX$

A full rank, known from the network structure

In practice: $Y = A'X + Z$

A' rank erasures

Z errors

Decoding possible if $\mathrm{rk}(A')$ not too small and $\mathrm{rk}(Z)$ not too big.

Rank metric: $d(X, Y) = \mathrm{rk}(X - Y)$

Rank metric codes

L/K finite field extension with basis $\alpha_1, \dots, \alpha_m$.

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

$$\begin{bmatrix} c_1 \\ c_2 \\ \vdots \\ c_m \end{bmatrix} \longleftrightarrow \begin{bmatrix} c \end{bmatrix}$$

$m(\mathbf{x}) \in K^{m \times n}$ $\qquad\qquad$ $\mathbf{x} \in L^n$

Rank metric code is subspace of $L^n \to$ subspace of $K^{m \times n}$.

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
$d_{R,r}$	generalized rank weight: minimum rank weight of subcode of dim r

Generalized rank weights

Oggier, Sboui (2012)

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

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)

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

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

Generalized rank weights

Oggier, Sboui (2012)

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

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)

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

J subspace of K^n

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

Lemma

$C(J)$ is a subspace of L^n

Proposition

If $L = \mathbb{F}_{q^m}$ and $K = \mathbb{F}_q$, then there is a $\mathbf{c} \in C$ such that

$$\mathrm{Rsupp}(\mathbf{c}) = \mathrm{Rsupp}(C).$$

Proof.

- True for any $\mathbf{c}$ in
$$C \setminus \bigcup_{\substack{\dim J = 1 \\ C(J) \neq C}} C(J).$$
- Nonempty by counting argument.

$\square$

Theorem (J, Pellikaan, 2015)

If $L = \mathbb{F}_{q^m}$ and $K = \mathbb{F}_q$, then

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

Remark: no idea for infinite fields.

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)

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

Galois closure and trace

$C \subseteq L^n$

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

Galois closure C^*: smallest space containing C, closed under $Gal(L/K)$

Galois closed: $C = C^*$

Subfield subcode $C|_K$: codewords with coefficients in K

$C \subseteq K^n$

Extension code $C \otimes L$: all L-linear combinations of words of C

Galois closure and trace

Theorem (Giorgetti, Previtali, 2010)

Let $C \subseteq L^n$. The following are equivalent:

- *C is Galois closed*
- *C has a basis over K^n*
- $C = Tr(C) \otimes L$
- $Tr(C) = C|_K$

$$\begin{tikzcd}
C \arrow[r, "Gal(L/K)"] \arrow[dr, "\mathrm{Tr}(\mathbf{c})"] & C^* & L \\
C|_K \arrow[u, hook] \arrow[r, hook] & \mathrm{Tr}(C) \arrow[u, "\otimes L"'] & K
\end{tikzcd}$$

Galois closure and trace

Theorem (J, Pellikaan, 2015)
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
$Rsupp(D) = Tr(D)$ *and* $wt_R(D) = \dim D^*$

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 (Ducoat, 2014; J, Pellikaan, 2015)

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

Proof.

- Let $V \subseteq L^n$ 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

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

□

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)

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

J, Pellikaan (2014)

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

C degenerate if $d_R(C^{\perp}) = 1$.

Proposition

C degenerate iff C rank equivalent with code that has last coordinate identically zero.

Theorem (J, Pellikaan, 2015)

C nondegenerate iff $Rsupp(C) = K^n$ iff $d_{R,k}(C) = n$.

Proof.

- Ducoat proved that for dual codes,

$$\{d_{R,r}(C) : r \in [k]\} = [n] \setminus \{n + 1 - d_{R,r}(C^{\perp}) : r \in [n-k]\}.$$

- So $d_{R,1}(C^{\perp}) = 1$ iff $d_{R,k}(C) < n$.

□

Summary

- Generalized rank weights are the rank metric equivalence of generalized Hamming weights.
- The three proposed definitions of the generalized rank weights are equivalent – at least over finite fields.
- When talking about Galois closure, one should also consider the trace function.
- As small application of generalized rank weights, on can prove things about degenerate codes.

Thank you for your attention.