Generalized weights of convolutional codes

Elisa Gorla
joint w/ Flavio Salizzoni

Institut de mathématiques, Université de Neuchâtel

Kloster Irsee, August 31, 2022

Convolutional codes

An (n, k, δ) **convolutional code** $\mathcal{C}$ is a non-zero $\mathbb{F}_q[x]$-submodule of rank k of $\mathbb{F}_q[x]^n$.

A **codeword** is a vector $c(x) = (p_1(x), \ldots, p_n(x)) \in \mathcal{C}$, $p_i(x) \in \mathbb{F}_q[x]$.

Convolutional codes

An (n, k, δ) **convolutional code** $\mathcal{C}$ is a non-zero $\mathbb{F}_q[x]$-submodule of rank k of $\mathbb{F}_q[x]^n$.

A **codeword** is a vector $c(x) = (p_1(x), \ldots, p_n(x)) \in \mathcal{C}$, $p_i(x) \in \mathbb{F}_q[x]$.

If $g_1(x), \ldots, g_k(x)$ is a basis of $\mathcal{C}$, then a **generator matrix** for $\mathcal{C}$ is

$$G(x) = \begin{pmatrix} g_1(x) \\ \vdots \\ g_k(x) \end{pmatrix}.$$

Assume $\deg(g_1(x)) \geq \deg(g_2(x)) \geq \ldots \deg(g_k(x))$.

The **internal degree** δ is the largest degree of a maximal minor of $G(x)$.

Convolutional codes

An (n, k, δ) **convolutional code** $\mathcal{C}$ is a non-zero $\mathbb{F}_q[x]$-submodule of rank k of $\mathbb{F}_q[x]^n$.

A **codeword** is a vector $c(x) = (p_1(x), \ldots, p_n(x)) \in \mathcal{C}$, $p_i(x) \in \mathbb{F}_q[x]$.

If $g_1(x), \ldots, g_k(x)$ is a basis of $\mathcal{C}$, then a **generator matrix** for $\mathcal{C}$ is

$$G(x) = \begin{pmatrix} g_1(x) \\ \vdots \\ g_k(x) \end{pmatrix}.$$

Assume $\deg(g_1(x)) \geq \deg(g_2(x)) \geq \ldots \deg(g_k(x))$.

The **internal degree** δ is the largest degree of a maximal minor of $G(x)$.

$\mathcal{C}$ is **non-catastrophic** if $G(x)$ has a right inverse with entries in $\mathbb{F}_q[x]$.

Support and weight

Definition

The **support** of $p(x) = \sum_{j=0}^{d} a_j x^j$ is $\operatorname{supp}(p(x)) = \{x^j \mid a_j \neq 0\}$.

The **support** of $c(x) = (p_1(x), \ldots, p_n(x)) \in \mathbb{F}_q[x]^n$, $p_i = \sum_{j=0}^{\deg(p_i)} a_{ij} x^j$, is

$$\operatorname{supp}(c(x)) = \{(\underbrace{0, \ldots, 0}_{i-1}, x^j, \underbrace{0, \ldots, 0}_{n-i}) \mid a_{ij} \neq 0\}.$$

The **weight** of $c(x)$ is $\operatorname{wt}(c(x)) = |\operatorname{supp}(c(x))|$.

Support and weight

Definition

The **support** of $p(x) = \sum_{j=0}^{d} a_j x^j$ is $\text{supp}(p(x)) = \{x^j \mid a_j \neq 0\}$.

The **support** of $c(x) = (p_1(x), \ldots, p_n(x)) \in \mathbb{F}_q[x]^n$, $p_i = \sum_{j=0}^{\deg(p_i)} a_{ij} x^j$, is

$$\text{supp}(c(x)) = \{(\underbrace{0, \ldots, 0}_{i-1}, x^j, \underbrace{0, \ldots, 0}_{n-i}) \mid a_{ij} \neq 0\}.$$

The **weight** of $c(x)$ is $\text{wt}(c(x)) = |\text{supp}(c(x))|$.

Example

$c(x) = (0, 1, 1 + x^2) \in \mathbb{F}_2[x]^3$ has
$\text{supp}(c(x)) = \{(0, 1, 0), (0, 0, 1), (0, 0, x^2)\}$ and $\text{wt}(c(x)) = 3$.

Support and weight

Definition

The **support** of $p(x) = \sum_{j=0}^{d} a_j x^j$ is $\text{supp}(p(x)) = \{x^j \mid a_j \neq 0\}$.

The **support** of $c(x) = (p_1(x), \dots, p_n(x)) \in \mathbb{F}_q[x]^n$, $p_i = \sum_{j=0}^{\deg(p_i)} a_{ij} x^j$, is

$$\text{supp}(c(x)) = \{(\underbrace{0, \dots, 0}_{i-1}, x^j, \underbrace{0, \dots, 0}_{n-i}) \mid a_{ij} \neq 0\}.$$

The **weight** of $c(x)$ is $\text{wt}(c(x)) = |\text{supp}(c(x))|$.

The **free distance** (or minimum distance) of $\mathcal{C}$ is

$$\text{d}_{\text{free}}(\mathcal{C}) = \min\{\text{wt}(c(x)) \mid c(x) \in \mathcal{C} \setminus \{0\}\}.$$

Example

$c(x) = (0, 1, 1 + x^2) \in \mathbb{F}_2[x]^3$ has
$\text{supp}(c(x)) = \{(0, 1, 0), (0, 0, 1), (0, 0, x^2)\}$ and $\text{wt}(c(x)) = 3$.

Support and weight

Definition

The **support** of $p(x) = \sum_{j=0}^{d} a_j x^j$ is $\text{supp}(p(x)) = \{x^j \mid a_j \neq 0\}$.

The **support** of $c(x) = (p_1(x), \ldots, p_n(x)) \in \mathbb{F}_q[x]^n$, $p_i = \sum_{j=0}^{\deg(p_i)} a_{ij} x^j$, is

$$\text{supp}(c(x)) = \{(\underbrace{0, \ldots, 0}_{i-1}, x^j, \underbrace{0, \ldots, 0}_{n-i}) \mid a_{ij} \neq 0\}.$$

The **weight** of $c(x)$ is $\text{wt}(c(x)) = |\text{supp}(c(x))|$.

The **free distance** (or minimum distance) of $\mathcal{C}$ is

$$\text{d}_{\text{free}}(\mathcal{C}) = \min\{\text{wt}(c(x)) \mid c(x) \in \mathcal{C} \setminus \{0\}\}.$$

Example

$c(x) = (0, 1, 1 + x^2) \in \mathbb{F}_2[x]^3$ has
$\text{supp}(c(x)) = \{(0,1,0), (0,0,1), (0,0,x^2)\}$ and $\text{wt}(c(x)) = 3$.

Generalized Hamming weights

Definition

A **linear block code** is a linear subspace $C \subseteq \mathbb{F}_q^n$.
The **Hamming support** of $c = (c_1, \ldots, c_n)$ is $\mathrm{supp}(c) = \{i \mid c_i \neq 0\}$.

This coincides with the support of c regarded as an element of $\mathbb{F}_q[x]^n$.

The **Hamming support** of $D \subseteq C$ is $\mathrm{supp}(D) = \bigcup_{c(x) \in D} \mathrm{supp}(c(x))$.

Generalized Hamming weights

Definition

A **linear block code** is a linear subspace $C \subseteq \mathbb{F}_q^n$.
The **Hamming support** of $c = (c_1, \ldots, c_n)$ is $\mathrm{supp}(c) = \{i \mid c_i \neq 0\}$.

This coincides with the support of c regarded as an element of $\mathbb{F}_q[x]^n$.

The **Hamming support** of $D \subseteq C$ is $\mathrm{supp}(D) = \bigcup_{c(x)\in D} \mathrm{supp}(c(x))$.

Definition (Helleseth, Kløve, Mykkeltveit)

The r-th **generalized (Hamming) weight** of $C \subseteq \mathbb{F}_q^n$ is

$$d_r^H(C) := \min\{|\mathrm{supp}(D)| : D \subseteq C, \dim(D) = r\}, \;\; 1 \leq r \leq \dim(C).$$

Generalized Hamming weights

Definition

A **linear block code** is a linear subspace $C \subseteq \mathbb{F}_q^n$.
The **Hamming support** of $c = (c_1, \dots, c_n)$ is $\mathrm{supp}(c) = \{i \mid c_i \neq 0\}$.

This coincides with the support of c regarded as an element of $\mathbb{F}_q[x]^n$.

The **Hamming support** of $D \subseteq C$ is $\mathrm{supp}(D) = \bigcup_{c(x) \in D} \mathrm{supp}(c(x))$.

Definition (Helleseth, Kløve, Mykkeltveit)

The r-th **generalized (Hamming) weight** of $C \subseteq \mathbb{F}_q^n$ is

$$d_r^H(C) := \min\{|\,\mathrm{supp}(D)| \,:\, D \subseteq C, \dim(D) = r\},\ \ 1 \leq r \leq \dim(C).$$

Generalized weights are invariants of codes, they sometimes allow us to distinguish nonequivalent codes. They measure worst-case security drops of a linear coding scheme for a wire-tap channel.

Generalized Hamming wts of conv'l codes

$\mathcal{C}$ an (n, k, δ) convolutional code.

The **support** of $D \subseteq \mathcal{C}$ is $\mathrm{supp}(D) = \bigcup_{c(x) \in D} \mathrm{supp}(c(x))$.

Definition (Rosenthal, York)

The r-th **generalized Hamming weight** of $\mathcal{C}$, $r \geq 1$

$$d_r^H(\mathcal{C}) = \min\{|\,\mathrm{supp}(D)| \,:\, D \subseteq \mathcal{C} \text{ an } \mathbb{F}_q\text{-linear subspace}, \dim(D) = r\}.$$

They amount to regarding $\mathcal{C} \subseteq \mathbb{F}_q[x]^n$ as a linear block code of infinite dimension and considering its generalized Hamming weights.

Generalized Hamming wts of conv'l codes

$\mathcal{C}$ an (n, k, δ) convolutional code.

The **support** of $D \subseteq \mathcal{C}$ is $\mathrm{supp}(D) = \bigcup_{c(x)\in D} \mathrm{supp}(c(x))$.

Definition (Rosenthal, York)

The r-th **generalized Hamming weight** of $\mathcal{C}$, $r \geq 1$

$$d_r^H(\mathcal{C}) = \min\{|\,\mathrm{supp}(D)| \;:\; D \subseteq \mathcal{C} \text{ an } \mathbb{F}_q\text{-linear subspace}, \dim(D) = r\}.$$

They amount to regarding $\mathcal{C} \subseteq \mathbb{F}_q[x]^n$ as a linear block code of infinite dimension and considering its generalized Hamming weights.

Properties (Wei - Rosenthal, York):

- $d_1^H(\mathcal{C}) = \mathrm{d}_{\mathrm{free}}(\mathcal{C})$,
- $d_r^H(\mathcal{C}) < d_{r+1}^H(\mathcal{C})$ for $r \geq 1$.

Example

Example

$\mathcal{C} = \langle (1,0,0),(0,1,1+x)\rangle_{\mathbb{F}_q[x]}$ has

- $D_1 = \langle (1,0,0)\rangle_{\mathbb{F}_q}$, $\mathrm{supp}(D_1) = \{(1,0,0)\} \rightsquigarrow d_1^H(\mathcal{C}) = 1$
- $D_2 = \langle (1,0,0),(x,0,0)\rangle_{\mathbb{F}_q}$,
  $\mathrm{supp}(D_2) = \{(1,0,0),(x,0,0,)\} \rightsquigarrow d_2^H(\mathcal{C}) = 2$
- $D_r = \langle (x^i,0,0) : 0 \leq i \leq r-1\rangle_{\mathbb{F}_q}$,
  $\mathrm{supp}(D_r) = \{(1,0,0),(x,0,0),\dots,(x^{r-1},0,0)\} \rightsquigarrow d_r^H(\mathcal{C}) = r$

Example

Example

$\mathcal{C} = \langle (1,0,0), (0,1,1+x) \rangle_{\mathbb{F}_q[x]}$ has

- $D_1 = \langle (1,0,0) \rangle_{\mathbb{F}_q}$, $\mathrm{supp}(D_1) = \{(1,0,0)\} \rightsquigarrow d_1^H(\mathcal{C}) = 1$
- $D_2 = \langle (1,0,0), (x,0,0) \rangle_{\mathbb{F}_q}$,
  $\mathrm{supp}(D_2) = \{(1,0,0), (x,0,0,)\} \rightsquigarrow d_2^H(\mathcal{C}) = 2$
- $D_r = \langle (x^i,0,0) : 0 \leq i \leq r-1 \rangle_{\mathbb{F}_q}$,
  $\mathrm{supp}(D_r) = \{(1,0,0), (x,0,0), \ldots, (x^{r-1},0,0)\} \rightsquigarrow d_r^H(\mathcal{C}) = r$

Remark

If a convolutional code $\mathcal{C}$ has $d_1^H(\mathcal{C}) = 1$, then $d_r^H(\mathcal{C}) = r$, for all $r \geq 1$.

Generalized weights of convolutional codes

$\mathcal{C}$ an (n, k, δ) convolutional code

Naive definition

The r-th **generalized weight** of $\mathcal{C}$, $1 \leq r \leq k = \mathrm{rk}(\mathcal{C})$

$$d_r(\mathcal{C}) = \min\{|\,\mathrm{supp}(\mathcal{D})| \,:\, \mathcal{D} \subseteq \mathcal{C} \text{ is a submodule of } \mathrm{rk}(\mathcal{D}) = r\}.$$

The **support** of $U \subseteq \mathcal{C}$ is $\mathrm{supp}(U) = \bigcup_{c(x) \in U} \mathrm{supp}(c(x))$.

Generalized weights of convolutional codes

$\mathcal{C}$ an (n, k, δ) convolutional code

Naive definition

The r-th **generalized weight** of $\mathcal{C}$, $1 \leq r \leq k = \text{rk}(\mathcal{C})$

$$d_r(\mathcal{C}) = \min\{|\,\text{supp}(\mathcal{D})| \;:\; \mathcal{D} \subseteq \mathcal{C} \text{ is a submodule of } \text{rk}(\mathcal{D}) = r\}.$$

The **support** of $U \subseteq \mathcal{C}$ is $\text{supp}(U) = \bigcup_{c(x)\in U} \text{supp}(c(x))$.

Rmk: If $\mathcal{D} \subseteq \mathcal{C}$ is a submodule, then $\text{supp}(\mathcal{D})$ has infinite cardinality.

Generalized weights of convolutional codes

$\mathcal{C}$ an (n, k, δ) convolutional code

Naive definition

The r-th **generalized weight** of $\mathcal{C}$, $1 \leq r \leq k = \mathrm{rk}(\mathcal{C})$

$$d_r(\mathcal{C}) = \min\{|\,\mathrm{supp}(\mathcal{D})| \,:\, \mathcal{D} \subseteq \mathcal{C} \text{ is a submodule of } \mathrm{rk}(\mathcal{D}) = r\}.$$

The **support** of $U \subseteq \mathcal{C}$ is $\mathrm{supp}(U) = \bigcup_{c(x) \in U} \mathrm{supp}(c(x))$.

Rmk: If $\mathcal{D} \subseteq \mathcal{C}$ is a submodule, then $\mathrm{supp}(\mathcal{D})$ has infinite cardinality.

Definition

The **weight** of $\mathcal{C}$ is

$$\mathrm{wt}(\mathcal{C}) = \min\{|\,\mathrm{supp}(\{g_1, \ldots, g_k\})| \,:\, g_1, \ldots, g_k \text{ are a basis of } \mathcal{C}\}.$$

Generalized weights of convolutional codes

$\mathcal{C}$ an (n, k, δ) convolutional code

Definition (G., Salizzoni)

The r-th **generalized weight** of $\mathcal{C}$, $1 \leq r \leq \mathrm{rk}(\mathcal{C})$

$$d_r(\mathcal{C}) = \min\{\mathrm{wt}(\mathcal{D}) \mid \mathcal{D} \subseteq \mathcal{C} \text{ is a submodule of } \mathrm{rk}(\mathcal{D}) = r\}.$$

The **support** of $U \subseteq \mathcal{C}$ is $\mathrm{supp}(U) = \bigcup_{c(x) \in U} \mathrm{supp}(c(x))$.

Rmk: If $\mathcal{D} \subseteq \mathcal{C}$ is a submodule, then $\mathrm{supp}(\mathcal{D})$ has infinite cardinality.

Definition

The **weight** of $\mathcal{C}$ is

$$\mathrm{wt}(\mathcal{C}) = \min\{|\,\mathrm{supp}(\{g_1, \ldots, g_k\})| \,:\, g_1, \ldots, g_k \text{ are a basis of } \mathcal{C}\}.$$

Example

$\mathcal{C}_1 = \langle (1,0,0),(0,1,1+x)\rangle_{\mathbb{F}_q[x]}$ has

- $\text{supp}(1,0,0) = \{(1,0,0)\}$ and $\text{wt}(\langle (1,0,0)\rangle_{\mathbb{F}_q[x]}) = 1 \quad \rightsquigarrow \quad d_1(\mathcal{C}_1) = 1$,
- $\text{supp}(1,0,0) \cup \text{supp}(0,1,1+x) = \{(1,0,0),(0,1,0),(0,0,1),(0,0,x)\}$ and $\text{wt}(\mathcal{C}_1) = 4 \quad \rightsquigarrow \quad d_2(\mathcal{C}_1) = 4$,
- $d_r^H(\mathcal{C}_1) = r$ for all $r \geq 1$.

Example

$\mathcal{C}_1 = \langle (1,0,0), (0,1,1+x) \rangle_{\mathbb{F}_q[x]}$ has

- $\mathrm{supp}(1,0,0) = \{(1,0,0)\}$ and $\mathrm{wt}(\langle (1,0,0) \rangle_{\mathbb{F}_q[x]}) = 1 \quad \rightsquigarrow \quad d_1(\mathcal{C}_1) = 1$,
- $\mathrm{supp}(1,0,0) \cup \mathrm{supp}(0,1,1+x) = \{(1,0,0), (0,1,0), (0,0,1), (0,0,x)\}$ and $\mathrm{wt}(\mathcal{C}_1) = 4 \quad \rightsquigarrow \quad d_2(\mathcal{C}_1) = 4$,
- $d_r^H(\mathcal{C}_1) = r$ for all $r \geq 1$.

Example

$\mathcal{C}_2 = \langle (1,0,0), (0,1,0) \rangle_{\mathbb{F}_q[x]}$ has

- $d_1(\mathcal{C}_2) = 1$ and $d_2(\mathcal{C}_2) = 2$,
- $d_r^H(\mathcal{C}_1) = r$ for all $r \geq 1$.

Example

$\mathcal{C}_1 = \langle (1,0,0), (0,1,1+x) \rangle_{\mathbb{F}_q[x]}$ has

- $\text{supp}(1,0,0) = \{(1,0,0)\}$ and $\text{wt}(\langle (1,0,0) \rangle_{\mathbb{F}_q[x]}) = 1 \quad \rightsquigarrow \quad d_1(\mathcal{C}_1) = 1$,
- $\text{supp}(1,0,0) \cup \text{supp}(0,1,1+x) = \{(1,0,0), (0,1,0), (0,0,1), (0,0,x)\}$ and $\text{wt}(\mathcal{C}_1) = 4 \quad \rightsquigarrow \quad d_2(\mathcal{C}_1) = 4$,
- $d_r^H(\mathcal{C}_1) = r$ for all $r \geq 1$.

Example

$\mathcal{C}_2 = \langle (1,0,0), (0,1,0) \rangle_{\mathbb{F}_q[x]}$ has

- $d_1(\mathcal{C}_2) = 1$ and $d_2(\mathcal{C}_2) = 2$,
- $d_r^H(\mathcal{C}_1) = r$ for all $r \geq 1$.

$\mathcal{C}_1$ and $\mathcal{C}_2$ can be distinguished by looking at d_1, d_2, but not d_1^H, d_2^H.

Generalized weights of linear block codes

$C \subseteq \mathbb{F}_q^n$ linear block code

$\mathcal{C} = C \otimes_{\mathbb{F}_q} \mathbb{F}_q[x] \subseteq \mathbb{F}_q[x]^n$ is a convolutional code with $\mathrm{rk}(\mathcal{C}) = \dim(C)$

Theorem (G., Salizzoni)

$d_r(\mathcal{C}) = d_r^H(C)$ *for* $1 \leq r \leq \dim(C)$

Generalized weights of linear block codes

$C \subseteq \mathbb{F}_q^n$ linear block code

$\mathcal{C} = C \otimes_{\mathbb{F}_q} \mathbb{F}_q[x] \subseteq \mathbb{F}_q[x]^n$ is a convolutional code with $\mathrm{rk}(\mathcal{C}) = \dim(C)$

Theorem (G., Salizzoni)

$d_r(\mathcal{C}) = d_r^H(C)$ *for* $1 \leq r \leq \dim(C)$

Example

$C = \langle (1,0,0),(0,1,1) \rangle_{\mathbb{F}_q} \subseteq \mathbb{F}_q^3$ has $\mathcal{C} = \langle (1,0,0),(0,1,1) \rangle_{\mathbb{F}_q[x]} \subseteq \mathbb{F}_q[x]^3$ and

- $d_1(\mathcal{C}) = d_1^H(C) = 1$ and $d_2(\mathcal{C}) = d_2^H(C) = 3$,
- $d_r^H(\mathcal{C}) = r$ for all $r \geq 1$.

In particular, $d_2^H(C) \neq d_2^H(\mathcal{C})$.

Basic properties

$\mathcal{D} \subseteq \mathcal{C} \subseteq \mathbb{F}_q[x]^n$ convolutional codes, $\mathrm{rk}(\mathcal{C}) = k$

- $d_1(\mathcal{C}) = \mathrm{d}_{\text{free}}(\mathcal{C})$,
- $d_1(\mathcal{C}) < d_2(\mathcal{C}) < \ldots < d_k(\mathcal{C})$,
- $d_r(\mathcal{D}) \geq d_r(\mathcal{C})$ for $1 \leq r \leq \mathrm{rk}(\mathcal{D})$,
- $d_k(\mathcal{C}) \leq n(\deg(g_1(x)) + 1)$,
- $d_r(\mathcal{C}) \leq n(\deg(g_1(x)) + 1) - k + r$ for $1 \leq r \leq k$,
- isometric codes have the same generalized weights.

Definition

$\mathcal{C}, \mathcal{D} \subseteq \mathbb{F}_q[x]^n$ convolutional codes are **isometric** if there is an isomorphism of $\mathbb{F}_q[x]$-modules $\varphi : \mathcal{C} \to \mathcal{D}$ such that $\mathrm{wt}(c(x)) = \mathrm{wt}(\varphi(c(x)))$ for all $c(x) \in \mathcal{C}$.

Duality

Definition

The **dual** of $\mathcal{C} \subseteq \mathbb{F}_q[x]^n$ is

$$\mathcal{C}^\perp = \{d(x) \in \mathbb{F}_q[x]^n \mid d(x) \cdot c(x) = 0 \text{ for all } c(x) \in \mathcal{C}\}.$$

Duality

Definition

The **dual** of $\mathcal{C} \subseteq \mathbb{F}_q[x]^n$ is

$$\mathcal{C}^\perp = \{d(x) \in \mathbb{F}_q[x]^n \mid d(x) \cdot c(x) = 0 \text{ for all } c(x) \in \mathcal{C}\}.$$

$\mathcal{C} \subseteq (\mathcal{C}^\perp)^\perp$. If $\mathcal{C}$ is non-catastrophic, then $(\mathcal{C}^\perp)^\perp = \mathcal{C}$.

Do the generalized weights of $\mathcal{C}$ determine those of $\mathcal{C}^\perp$?

Duality

Definition

The **dual** of $\mathcal{C} \subseteq \mathbb{F}_q[x]^n$ is

$$\mathcal{C}^\perp = \{d(x) \in \mathbb{F}_q[x]^n \mid d(x) \cdot c(x) = 0 \text{ for all } c(x) \in \mathcal{C}\}.$$

$\mathcal{C} \subseteq (\mathcal{C}^\perp)^\perp$. If $\mathcal{C}$ is non-catastrophic, then $(\mathcal{C}^\perp)^\perp = \mathcal{C}$.

Do the generalized weights of $\mathcal{C}$ determine those of $\mathcal{C}^\perp$?

Example

$\mathcal{C}_1 = \langle(1+x, 1+x, 1, 0)\rangle_{\mathbb{F}_q[x]}, \mathcal{C}_2 = \langle(1+x, 1, 1, 1)\rangle_{\mathbb{F}_q[x]}$ have $d_1(\mathcal{C}_1) = d_1(\mathcal{C}_2) = 5$, but $d_1(\mathcal{C}_1^\perp) = 1$ and $d_1(\mathcal{C}_2^\perp) = 2$.

Duality

Definition

The **dual** of $\mathcal{C} \subseteq \mathbb{F}_q[x]^n$ is

$$\mathcal{C}^\perp = \{d(x) \in \mathbb{F}_q[x]^n \mid d(x) \cdot c(x) = 0 \text{ for all } c(x) \in \mathcal{C}\}.$$

$\mathcal{C} \subseteq (\mathcal{C}^\perp)^\perp$. If $\mathcal{C}$ is non-catastrophic, then $(\mathcal{C}^\perp)^\perp = \mathcal{C}$.

Do the generalized weights of $\mathcal{C}$ determine those of $\mathcal{C}^\perp$?

Example

$\mathcal{C}_1 = \langle (1+x, 1+x, 1, 0) \rangle_{\mathbb{F}_q[x]}, \mathcal{C}_2 = \langle (1+x, 1, 1, 1) \rangle_{\mathbb{F}_q[x]}$ have $d_1(\mathcal{C}_1) = d_1(\mathcal{C}_2) = 5$, but $d_1(\mathcal{C}_1^\perp) = 1$ and $d_1(\mathcal{C}_2^\perp) = 2$.

Proposition (G., Salizzoni)

$C \subseteq \mathbb{F}_q^n$ linear block code, $\mathcal{C} = C \otimes_{\mathbb{F}_q} \mathbb{F}_q[x] \subseteq \mathbb{F}_q[x]^n$.
The generalized weights of $\mathcal{C}$ determine those of $\mathcal{C}^\perp$.

The reverse code

Definition

The **reverse** of $c(x) \in \mathbb{F}_q[x]^n \setminus \{0\}$ is $\mathrm{rev}(c(x)) = x^{\deg(c(x))} c\left(\frac{1}{x}\right)$.

Example

$c(x) = (x^2 + 2x + 3, 1, 2x + 1) \in \mathbb{F}_5[x]^3$, $\deg(c(x)) = 2$ and

$$\mathrm{rev}(c(x)) = x^2 \left(\frac{1}{x^2} + \frac{2}{x} + 3, 1, \frac{2}{x} + 1 \right) = (1 + 2x + 3x^2, x^2, 2x + x^2).$$

The reverse code

Definition

The **reverse** of $c(x) \in \mathbb{F}_q[x]^n \setminus \{0\}$ is $\mathrm{rev}(c(x)) = x^{\deg(c(x))} c\left(\frac{1}{x}\right)$.

The **reverse code** of $\mathcal{C} \subseteq \mathbb{F}_q[x]^n$ is

$$\mathrm{rev}(\mathcal{C}) = \langle \mathrm{rev}(c(x)) \mid c(x) \in \mathcal{C} \setminus \{0\} \rangle_{\mathbb{F}_q[x]}.$$

Example

$c(x) = (x^2 + 2x + 3, 1, 2x + 1) \in \mathbb{F}_5[x]^3$, $\deg(c(x)) = 2$ and

$$\mathrm{rev}(c(x)) = x^2 \left(\frac{1}{x^2} + \frac{2}{x} + 3, 1, \frac{2}{x} + 1 \right) = (1 + 2x + 3x^2, x^2, 2x + x^2).$$

The reverse code

Definition

The **reverse** of $c(x) \in \mathbb{F}_q[x]^n \setminus \{0\}$ is $\mathrm{rev}(c(x)) = x^{\deg(c(x))} c\left(\frac{1}{x}\right)$.

The **reverse code** of $\mathcal{C} \subseteq \mathbb{F}_q[x]^n$ is

$$\mathrm{rev}(\mathcal{C}) = \langle \mathrm{rev}(c(x)) \mid c(x) \in \mathcal{C} \setminus \{0\} \rangle_{\mathbb{F}_q[x]}.$$

Example

$c(x) = (x^2 + 2x + 3, 1, 2x + 1) \in \mathbb{F}_5[x]^3$, $\deg(c(x)) = 2$ and

$$\mathrm{rev}(c(x)) = x^2 \left(\frac{1}{x^2} + \frac{2}{x} + 3, 1, \frac{2}{x} + 1 \right) = (1 + 2x + 3x^2, x^2, 2x + x^2).$$

Theorem (G., Salizzoni)

$d_r(\mathcal{C}) = d_r(\mathrm{rev}(\mathcal{C}))$ *for* $1 \leq r \leq \mathrm{rk}(\mathcal{C})$

MDS convolutional codes

$\mathcal{C}$ an (n, k, δ) convolutional code

Theorem (Singleton bound – Rosenthal, Smarandache)

$$\mathrm{d}_{\mathsf{free}}(\mathcal{C}) \leq (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1.$$

Definition

A **Maximum Distance Separable (MDS)** code is a code that meets the Singleton bound.

MDS convolutional codes

$\mathcal{C}$ an (n, k, δ) convolutional code

Theorem (Singleton bound – Rosenthal, Smarandache)

$$\mathrm{d}_{\mathrm{free}}(\mathcal{C}) \leq (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + 1.$$

Definition

A **Maximum Distance Separable (MDS)** code is a code that meets the Singleton bound.

Theorem (G., Salizzoni)

Let $\mathcal{C}$ be an (n, k, δ) MDS convolutional code, $1 \leq r \leq k$.

- *If $k = n$, then $d_r(\mathcal{C}) = \delta + r$.*
- *If $k \mid \delta$, then $d_r(\mathcal{C}) = (n-k)\left(\frac{\delta}{k} + 1\right) + \delta + r$.*
- *If $k \nmid \delta$, then $d_r(\mathcal{C}) \leq (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 2\right) + \delta + r$.*

Example

Let $n = 3, k = 2, \delta = 1$. If $\mathcal{C}$ is MDS, then

- $d_1(\mathcal{C}) = \mathrm{d}_{\mathrm{free}}(\mathcal{C}) = 3$,
- $4 = d_1(\mathcal{C}) + 1 \leq d_2(\mathcal{C}) \leq (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 2\right) + \delta + k = 5.$

Example

Let $n = 3, k = 2, \delta = 1$. If $\mathcal{C}$ is MDS, then

- $d_1(\mathcal{C}) = \mathrm{d}_{\mathrm{free}}(\mathcal{C}) = 3$,
- $4 = d_1(\mathcal{C}) + 1 \leq d_2(\mathcal{C}) \leq (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 2\right) + \delta + k = 5$.

Consider the two $(3, 2, 1)$ MDS convolutional codes:

$$\mathcal{C}_1 = \langle (2x, x+1, x+1), (1, 1, 2) \rangle_{\mathbb{F}_q[x]}$$
$$\mathcal{C}_2 = \langle (2x, x+1, 0), (1, 1, 2) \rangle_{\mathbb{F}_q[x]}$$

Example

Let $n = 3, k = 2, \delta = 1$. If $\mathcal{C}$ is MDS, then

- $d_1(\mathcal{C}) = \mathrm{d}_{\text{free}}(\mathcal{C}) = 3$,
- $4 = d_1(\mathcal{C}) + 1 \leq d_2(\mathcal{C}) \leq (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 2\right) + \delta + k = 5$.

Consider the two $(3, 2, 1)$ MDS convolutional codes:

$$\mathcal{C}_1 = \langle (2x, x+1, x+1), (1, 1, 2) \rangle_{\mathbb{F}_q[x]}$$
$$\mathcal{C}_2 = \langle (2x, x+1, 0), (1, 1, 2) \rangle_{\mathbb{F}_q[x]}$$

- $d_1(\mathcal{C}_1) = d_1(\mathcal{C}_2) = 3$,
- $d_2(\mathcal{C}_1) = 5$, while $d_2(\mathcal{C}_2) = 4$.

A (sometimes) tighter bound

$\mathcal{C} \subseteq \mathbb{F}_q[x]^n \rightsquigarrow \mathcal{C}[0] = \{c(0) \mid c(x) \in \mathcal{C}\} \subseteq \mathbb{F}_q^n$ linear block code

Theorem (G., Salizzoni)

$\mathcal{C}$ an (n, k, δ) MDS convolutional code, $\delta = k\left\lceil \frac{\delta}{k} \right\rceil - a$ with $0 < a < k$. Then

$$d_r(\mathcal{C}) = (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + r \text{ for } 1 \le r \le a$$

and

$$d_{a+r}(\mathcal{C}) \le (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + a + \min\left\{d_r^H(\mathcal{C}[0]), d_r^H(\mathrm{rev}(\mathcal{C})[0])\right\}$$

for $1 \le r \le k - a$.

A (sometimes) tighter bound

$\mathcal{C} \subseteq \mathbb{F}_q[x]^n \rightsquigarrow \mathcal{C}[0] = \{c(0) \mid c(x) \in \mathcal{C}\} \subseteq \mathbb{F}_q^n$ linear block code

Theorem (G., Salizzoni)

$\mathcal{C}$ an (n, k, δ) MDS convolutional code, $\delta = k\left\lceil \frac{\delta}{k} \right\rceil - a$ with $0 < a < k$. Then

$$d_r(\mathcal{C}) = (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + r \text{ for } 1 \leq r \leq a$$

and

$$d_{a+r}(\mathcal{C}) \leq (n-k)\left(\left\lfloor \frac{\delta}{k} \right\rfloor + 1\right) + \delta + a + \min\left\{d_r^H(\mathcal{C}[0]), d_r^H(\mathrm{rev}(\mathcal{C})[0])\right\}$$

for $1 \leq r \leq k - a$.

Question: Can this bound be improved?

Anticode bound

Definition

$\mathcal{C}$ an (n, k, δ) convolutional code, $D \subseteq \mathcal{C}$ an $\mathbb{F}_q$-linear subspace

$$\mathrm{maxwt}(D) = \max\{\mathrm{wt}(d(x)) \mid d(x) \in D\}$$

Anticode bound

Definition

$\mathcal{C}$ an (n, k, δ) convolutional code, $D \subseteq \mathcal{C}$ an $\mathbb{F}_q$-linear subspace

$$\mathrm{maxwt}(D) = \max\{\mathrm{wt}(d(x)) \mid d(x) \in D\}$$

$$\mathrm{maxwt}(\mathcal{C}) = \min\{\mathrm{maxwt}(D) \mid \dim(D) = \mathrm{rk}(D \otimes_{\mathbb{F}_q} \mathbb{F}_q[x]) = k\}$$

Anticode bound

Definition

$\mathcal{C}$ an (n, k, δ) convolutional code, $D \subseteq \mathcal{C}$ an $\mathbb{F}_q$-linear subspace

$$\text{maxwt}(D) = \max\{\text{wt}(d(x)) \mid d(x) \in D\}$$

$$\text{maxwt}(\mathcal{C}) = \min\{\text{maxwt}(D) \mid \dim(D) = \text{rk}(D \otimes_{\mathbb{F}_q} \mathbb{F}_q[x]) = k\}$$

Example

$\mathcal{C} = \langle (1,1,0), (0,1,1) \rangle_{\mathbb{F}_2[x]} \subseteq \mathbb{F}_2[x]^3$,

$D_1 = \langle (1,1,0), (0,1,1) \rangle_{\mathbb{F}_2}$, $D_2 = \langle (1,1,0), (0,x,x) \rangle_{\mathbb{F}_2}$

have $\text{maxwt}(D_1) = 2$ and $\text{maxwt}(D_2) = 4$.

Anticode bound

Definition

$\mathcal{C}$ an (n,k,δ) convolutional code, $D \subseteq \mathcal{C}$ an $\mathbb{F}_q$-linear subspace

$$\mathrm{maxwt}(D) = \max\{\mathrm{wt}(d(x)) \mid d(x) \in D\}$$

$$\mathrm{maxwt}(\mathcal{C}) = \min\{\mathrm{maxwt}(D) \mid \dim(D) = \mathrm{rk}(D \otimes_{\mathbb{F}_q} \mathbb{F}_q[x]) = k\}$$

Example

$\mathcal{C} = \langle (1,1,0),(0,1,1) \rangle_{\mathbb{F}_2[x]} \subseteq \mathbb{F}_2[x]^3$,
$D_1 = \langle (1,1,0),(0,1,1) \rangle_{\mathbb{F}_2}$, $D_2 = \langle (1,1,0),(0,x,x) \rangle_{\mathbb{F}_2}$
have $\mathrm{maxwt}(D_1) = 2$ and $\mathrm{maxwt}(D_2) = 4$.

Theorem (Anticode bound – G., Salizzoni)

$$\mathrm{rk}(\mathcal{C}) \leq \mathrm{maxwt}(\mathcal{C})$$

Optimal anticodes

Definition

An **optimal anticode** is a code that meets the anticode bound.

Optimal anticodes

Definition

An **optimal anticode** is a code that meets the anticode bound.

Example

$\mathcal{C} = \langle (1,1,0),(0,1,1)\rangle_{\mathbb{F}_2[x]} \subseteq \mathbb{F}_2[x]^3$ is an optimal anticode, since $C = \langle (1,1,0),(0,1,1)\rangle_{\mathbb{F}_2}$ has $\dim(C) = \mathrm{maxwt}(C) = 2$ and $C \otimes_{\mathbb{F}_2} \mathbb{F}_2[x] = \mathcal{C}$.

Optimal anticodes

Definition

An **optimal anticode** is a code that meets the anticode bound.

Example

$\mathcal{C} = \langle (1,1,0), (0,1,1) \rangle_{\mathbb{F}_2[x]} \subseteq \mathbb{F}_2[x]^3$ is an optimal anticode, since $C = \langle (1,1,0), (0,1,1) \rangle_{\mathbb{F}_2}$ has $\dim(C) = \text{maxwt}(C) = 2$ and $C \otimes_{\mathbb{F}_2} \mathbb{F}_2[x] = \mathcal{C}$.

Theorem (G., Salizzoni)

$\mathcal{C}$ an (n, k, δ) convolutional code.

- *If $d_r(\mathcal{C}) = r$ for $1 \leq r \leq k$, then $\mathcal{C}$ is an optimal anticode.*
- *If $\mathcal{C}$ is an optimal anticode and $q \neq 2$, then $d_r(\mathcal{C}) = r$ for $1 \leq r \leq k$.*

Optimal anticodes

Definition

An **optimal anticode** is a code that meets the anticode bound.

Example

$\mathcal{C} = \langle (1,1,0),(0,1,1)\rangle_{\mathbb{F}_2[x]} \subseteq \mathbb{F}_2[x]^3$ is an optimal anticode, since $C = \langle (1,1,0),(0,1,1)\rangle_{\mathbb{F}_2}$ has $\dim(C) = \mathrm{maxwt}(C) = 2$ and $C \otimes_{\mathbb{F}_2} \mathbb{F}_2[x] = \mathcal{C}$. However, $d_1(\mathcal{C}) = 2$, $d_2(\mathcal{C}) = 3$.

Theorem (G., Salizzoni)

$\mathcal{C}$ an (n,k,δ) convolutional code.

- *If $d_r(\mathcal{C}) = r$ for $1 \leq r \leq k$, then $\mathcal{C}$ is an optimal anticode.*
- *If $\mathcal{C}$ is an optimal anticode and $q \neq 2$, then $d_r(\mathcal{C}) = r$ for $1 \leq r \leq k$.*

Elementary optimal anticodes

Example

A code in $\mathbb{F}_q[x]^n$ with basis elements of the form $(0, \ldots, 0, x^j, 0, \ldots, 0)$ is an optimal anticode, which we call **elementary optimal anticode**.

Elementary optimal anticodes

Example

A code in $\mathbb{F}_q[x]^n$ with basis elements of the form $(0,\ldots,0,x^j,0,\ldots,0)$ is an optimal anticode, which we call **elementary optimal anticode**.

Example

$\mathcal{C} = \langle (1,x),(x,0)\rangle_{\mathbb{F}_q[x]}$ is an optimal anticode, but not an elementary optimal anticode.

$\mathcal{C} \supseteq \langle (0,x^2),(x,0)\rangle_{\mathbb{F}_q[x]}$ an elementary optimal anticode.

Elementary optimal anticodes

Example

A code in $\mathbb{F}_q[x]^n$ with basis elements of the form $(0,\ldots,0,x^j,0,\ldots,0)$ is an optimal anticode, which we call **elementary optimal anticode**.

Example

$\mathcal{C} = \langle (1,x),(x,0)\rangle_{\mathbb{F}_q[x]}$ is an optimal anticode, but not an elementary optimal anticode.

$\mathcal{C} \supseteq \langle (0,x^2),(x,0)\rangle_{\mathbb{F}_q[x]}$ an elementary optimal anticode.

Theorem (G., Salizzoni)

$\mathcal{C}$ an (n,k,δ) convolutional code. $\mathcal{C}$ is an optimal anticode if and only if there exists an elementary optimal anticode $\mathcal{A} \subseteq \mathcal{C}$ s.t. $\mathrm{rk}(\mathcal{A}) = k$.

Duality

Theorem (G., Salizzoni)

Let $q \neq 2$. The dual code of an optimal anticode is an elementary optimal anticode generated by vectors of the standard basis of $\mathbb{F}_q^n$.

Duality

Theorem (G., Salizzoni)

Let $q \neq 2$. The dual code of an optimal anticode is an elementary optimal anticode generated by vectors of the standard basis of $\mathbb{F}_q^n$.

Example

$\mathcal{C} = \langle (1,1,0),(0,1,1) \rangle_{\mathbb{F}_2[x]} \subseteq \mathbb{F}_2[x]^3$ is an optimal anticode, while
$\mathcal{C}^\perp = \langle (1,1,1) \rangle_{\mathbb{F}_2[x]} \subseteq \mathbb{F}_2[x]^3$ is not an optimal anticode.

Duality

Theorem (G., Salizzoni)

Let $q \neq 2$. The dual code of an optimal anticode is an elementary optimal anticode generated by vectors of the standard basis of $\mathbb{F}_q^n$.

Example

$\mathcal{C} = \langle (1,1,0),(0,1,1) \rangle_{\mathbb{F}_2[x]} \subseteq \mathbb{F}_2[x]^3$ is an optimal anticode, while
$\mathcal{C}^\perp = \langle (1,1,1) \rangle_{\mathbb{F}_2[x]} \subseteq \mathbb{F}_2[x]^3$ is not an optimal anticode.

Theorem (G., Salizzoni)

$C \subseteq \mathbb{F}_q^n$ a linear block code, $\mathcal{C} = C \otimes_{\mathbb{F}_q} \mathbb{F}_q[x] \subseteq \mathbb{F}_q[x]^n$.
C is an optimal anticode if and only if $\mathcal{C}$ is an optimal anticode.

The pathologies for $q = 2$ come directly from linear block codes.

Duality

Theorem (G., Salizzoni)

Let $q \neq 2$. The dual code of an optimal anticode is an elementary optimal anticode generated by vectors of the standard basis of $\mathbb{F}_q^n$.

Example

$\mathcal{C} = \langle(1,1,0),(0,1,1)\rangle_{\mathbb{F}_2[x]} \subseteq \mathbb{F}_2[x]^3$ is an optimal anticode, while
$\mathcal{C}^\perp = \langle(1,1,1)\rangle_{\mathbb{F}_2[x]} \subseteq \mathbb{F}_2[x]^3$ is not an optimal anticode.

Theorem (G., Salizzoni)

$C \subseteq \mathbb{F}_q^n$ a linear block code, $\mathcal{C} = C \otimes_{\mathbb{F}_q} \mathbb{F}_q[x] \subseteq \mathbb{F}_q[x]^n$.
C is an optimal anticode if and only if $\mathcal{C}$ is an optimal anticode.

The pathologies for $q = 2$ come directly from linear block codes.

Thank you for your attention!