The small weight words of some Hermitian codes

Chiara Marcolla

University of Trento, Italy
Department of Mathematics

Cork, Workshop on Coding and Cryptography

The small weight words of some Hermitian codes

The small weight words of some Hermitian codes

Acknowledgements

The work is jointly with Marco Pellegrini and our supervisor Massimiliano Sala.

The small weight words of some Hermitian codes

Hermitian curve

We consider the Hermitian curve χ over $\mathbb{F}_{q^2}$

$$x^{q+1} = y^q + y$$

The norm is a function $N : \mathbb{F}_{q^r} \to \mathbb{F}_q$ such that

$$N(x) = x^{1+q+\cdots+q^{r-1}}$$

The trace is a function $Tr : \mathbb{F}_{q^r} \to \mathbb{F}_q$ such that

$$Tr(x) = x + x^q + \cdots + x^{q^{r-1}}$$

Hermitian curve

We consider the Hermitian curve χ over $\mathbb{F}_{q^2}$

$$x^{q+1} = y^q + y$$

The norm is a function $N : \mathbb{F}_{q^r} \to \mathbb{F}_q$ such that

$$N(x) = x^{1+q+\cdots+q^{r-1}}$$

The trace is a function $Tr : \mathbb{F}_{q^r} \to \mathbb{F}_q$ such that

$$Tr(x) = x + x^q + \cdots + x^{q^{r-1}}$$

Hermitian curve

The Hermitian curve can be described as

$$N(x) = Tr(y), \quad \text{with } r = 2$$

This curve has exactly

$$n = (q^2 \text{ of } x) \cdot (q \text{ of } y) = q^3 \text{ rational points}$$

that we call $\mathcal{P} = \{P_1, \ldots, P_n\}$.

Hermitian curve

The Hermitian curve can be described as

$$N(x) = Tr(y), \quad \text{with } r = 2$$

This curve has exactly

$$n = (q^2 \text{ of } x) \cdot (q \text{ of } y) = q^3 \text{ rational points}$$

that we call $\mathcal{P} = \{P_1, \dots, P_n\}$.

Hermitian code

Definition

The evaluation map is

$$ev_{\mathcal{P}} : \mathbb{F}_q[x,y]/\langle x^{q+1} - y^q - y\rangle \longrightarrow (\mathbb{F}_{q^2})^n$$

$$ev_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n))$$

Let m be a natural number, then we define

$$\mathcal{B}_{m,q} = \{x^r y^s \mid \mathrm{w}(x^r y^s) \leq m,\ 0 \leq s \leq q-1\}$$

So we consider

$$E_m = \langle ev_{\mathcal{P}}(f) \text{ such that } f \in \mathcal{B}_{m,q}\rangle$$

Hermitian code

Definition

The evaluation map is

$$ev_{\mathcal{P}} : \mathbb{F}_q[x, y]/\langle x^{q+1} - y^q - y \rangle \longrightarrow (\mathbb{F}_{q^2})^n$$

$$ev_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n))$$

Let m be a natural number, then we define

$$\mathcal{B}_{m,q} = \{x^r y^s \mid \mathrm{w}(x^r y^s) \leq m,\ 0 \leq s \leq q-1\}$$

So we consider

$$E_m = \langle ev_{\mathcal{P}}(f) \text{ such that } f \in \mathcal{B}_{m,q} \rangle$$

Hermitian code

Definition

The evaluation map is

$$ev_{\mathcal{P}} : \mathbb{F}_q[x,y]/\langle x^{q+1} - y^q - y \rangle \longrightarrow (\mathbb{F}_{q^2})^n$$

$$ev_{\mathcal{P}}(f) = (f(P_1), \ldots, f(P_n))$$

Let m be a natural number, then we define

$$\mathcal{B}_{m,q} = \{x^r y^s \mid \mathrm{w}(x^r y^s) \leq m,\ 0 \leq s \leq q-1\}$$

So we consider

$$E_m = \langle ev_{\mathcal{P}}(f) \text{ such that } f \in \mathcal{B}_{m,q} \rangle$$

Hermitian code

Therefore

$$C_m = (E_m)^{\perp} = \{\mathbf{c} \in (\mathbb{F}_q)^n \mid \mathbf{c} \cdot ev_{\mathcal{P}}(f) = 0 \text{ and } f \in \mathcal{B}_{m,q}\}$$

$C(m,q) = C_m$ is called Hermitian code. The parity-check matrix $\mathbf{H}$ of $C(m,q)$ is

$$\mathbf{H} = \begin{pmatrix} f_1(P_1) & \dots & f_1(P_n) \\ \vdots & \ddots & \vdots \\ f_i(P_1) & \dots & f_i(P_n) \end{pmatrix}$$

where $f_j \in \mathcal{B}_{m,q}$.

Hermitian code

Therefore

$$C_m = (E_m)^{\perp} = \{\mathbf{c} \in (\mathbb{F}_q)^n \mid \mathbf{c} \cdot ev_{\mathcal{P}}(f) = 0 \text{ and } f \in \mathcal{B}_{m,q}\}$$

$C(m,q) = C_m$ is called Hermitian code. The parity-check matrix **H** of $C(m,q)$ is

$$\mathbf{H} = \begin{pmatrix} f_1(P_1) & \dots & f_1(P_n) \\ \vdots & \ddots & \vdots \\ f_i(P_1) & \dots & f_i(P_n) \end{pmatrix}$$

where $f_j \in \mathcal{B}_{m,q}$.

The four phases of Hermitian codes

Phase	m
1	$0 \leq m \leq q^2 - q - 2$
2	$q^2 - q \leq m \leq 2q^2 - 2q - 2$
3	$2q^2 - 2q - 1 \leq m \leq q^3 - 1$
4	$q^3 \leq m < q^3 + q^2 - q - 1$

We have studied phase one, i.e. the case $d \leq q$.

The small weight words of some Hermitian codes

Corner Code

If **H** is composed of (the evaluation of) these sets

$$\begin{aligned} L_0^d &= \{1, x, \dots, x^{d-2}\} \\ L_1^d &= \{y, xy, \dots, x^{d-3}y\} \\ &\vdots \\ L_{d-2}^d &= \{y^{d-2}\} \end{aligned}$$

Then the code is called a Corner Code and it is indicated H_d^0.
The dimension of this code is

$$k = n - \frac{d(d-1)}{2}.$$

Edge Code

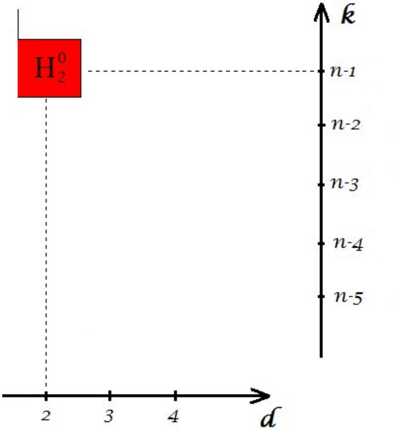
The code having parity-check matrix composed of $L_0^d \sqcup \cdots \sqcup L_{d-2}^d$ and of

$$\begin{aligned} l_1^d &= x^{d-1} \\ l_2^d &= x^{d-2}y \\ &\vdots \\ l_j^d &= x^{d-j}y^{j-1} \end{aligned}$$

is called an Edge Code, denoted with H_d^j $(1 \leq j \leq d-1)$.
The dimension of this code is

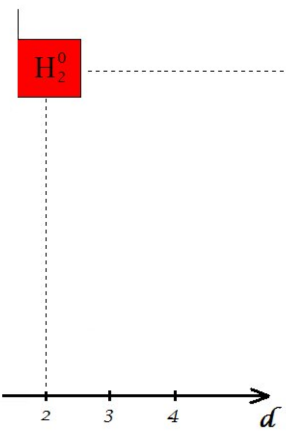
$$k = n - \frac{d(d-1)}{2} - j.$$

Corner Code e Edge Code



- $\mathbf{H}_{\mathbf{2}}^{\mathbf{0}}$ is $[n, n-1, 2]$ code. $\mathcal{B}_{m,q} = L_0^2 = \{1\}$.

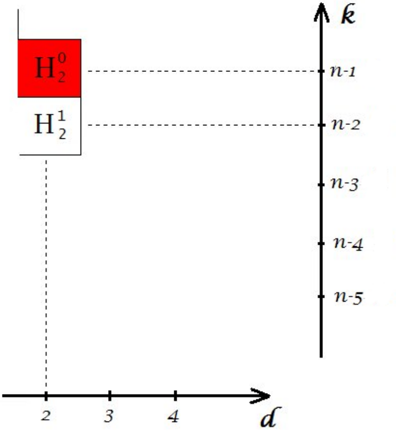
Corner Code e Edge Code



- H_2^0 is $[n, n-1, 2]$ code.
  $\mathcal{B}_{m,q} = L_0^2 = \{1\}$.

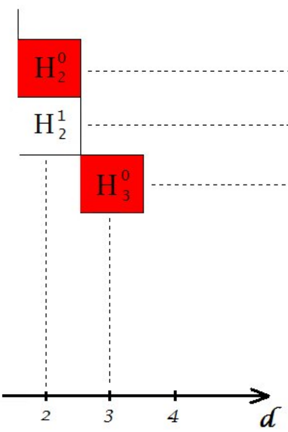
$$L_0^d = \{1, x, \dots, x^{d-2}\}$$
$$L_1^d = \{y, xy, \dots, x^{d-3}y\}$$
$$\vdots$$
$$L_{d-2}^d = \{y^{d-2}\}$$

Corner Code e Edge Code



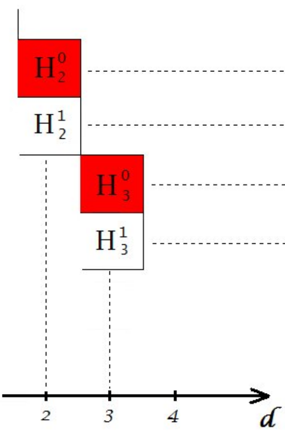
- H_2^0 is $[n, n-1, 2]$ code.
  $\mathcal{B}_{m,q} = L_0^2 = \{1\}$.
- H_2^1 is $[n, n-2, 2]$ code.
  $\mathcal{B}_{m,q} = L_0^2 \sqcup l_1^2 = \{1, x\}$

Corner Code e Edge Code



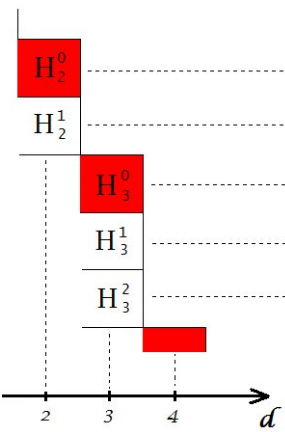
- $\mathrm{H}_{\mathbf{2}}^{\mathbf{0}}$ is $[n, n-1, 2]$ code.
  $\mathcal{B}_{m,q} = L_0^2 = \{1\}$.
- $\mathrm{H}_{\mathbf{2}}^{\mathbf{1}}$ is $[n, n-2, 2]$ code.
  $\mathcal{B}_{m,q} = L_0^2 \sqcup I_1^2 = \{1, x\}$
- $\mathrm{H}_{\mathbf{3}}^{\mathbf{0}}$ is $[n, n-3, 3]$ code.
  $\mathcal{B}_{m,q} = L_0^3 \sqcup L_1^3 = \{1, x, y\}$

Corner Code e Edge Code



- H_2^0 is $[n, n-1, 2]$ code. $\mathcal{B}_{m,q} = L_0^2 = \{1\}$.
- H_2^1 is $[n, n-2, 2]$ code. $\mathcal{B}_{m,q} = L_0^2 \sqcup l_1^2 = \{1, x\}$
- H_3^0 is $[n, n-3, 3]$ code. $\mathcal{B}_{m,q} = L_0^3 \sqcup L_1^3 = \{1, x, y\}$
- H_3^1 is $[n, n-4, 3]$ code. $\mathcal{B}_{m,q} = L_0^3 \sqcup L_1^3 \sqcup l_1^3 = \{1, x, y, x^2\}$

Corner Code e Edge Code



- H_2^0 is $[n, n-1, 2]$ code. $\mathcal{B}_{m,q} = L_0^2 = \{1\}$.
- H_2^1 is $[n, n-2, 2]$ code. $\mathcal{B}_{m,q} = L_0^2 \sqcup l_1^2 = \{1, x\}$
- H_3^0 is $[n, n-3, 3]$ code. $\mathcal{B}_{m,q} = L_0^3 \sqcup L_1^3 = \{1, x, y\}$
- H_3^1 is $[n, n-4, 3]$ code. $\mathcal{B}_{m,q} = L_0^3 \sqcup L_1^3 \sqcup l_1^3 = \{1, x, y, x^2\}$
- H_3^2 is $[n, n-5, 3]$ code. $\mathcal{B}_{m,q} = L_0^3 \sqcup L_1^3 \sqcup \{l_1^3, l_2^3\} = \{1, x, y, x^2, xy\}$

The number of codewords

Let $C(m,q) = \mathcal{C}_{m,q}$ be an Hermitian code. So

$$z \in \mathcal{C}_{m,q} \iff z\mathbf{H} = 0$$

$$\sum_{i=1}^{n} z_i f_j(P_i) = 0 \quad \forall j = 1,\ldots,n-k \text{ for } f_j \in \mathcal{B}_{m,q} = \{f_1,\ldots,f_{n-k}\}$$

All words of weight w correspond to solutions of this system:

$$J_{q,m}(w) = \begin{cases} \sum_{i=1}^{w} z_i x_i^r y_i^s = 0 \quad \forall\, r,s \quad \text{for} \quad x^r y^s \in \mathcal{B}_{m,q} \\ x_i^{q+1} - y_i^q - y_i = 0 \quad \forall\, i = 1,\ldots,w \\ x_i^{q^2} - x_i = 0 \quad y_i^{q^2} - y_i = 0 \quad z_i^{q^2-1} - 1 = 0 \quad \forall\, i = 1,\ldots,w \\ \prod_{1 \le i < j \le w}((x_i - x_j)^{q^2-1} - 1)((y_i - y_j)^{q^2-1} - 1) = 0 \end{cases}$$

$$A_w(\mathcal{C}_{m,q}(w)) = \frac{|\mathcal{V}(J_{q,m}(w))|}{w!}$$

The number of codewords

Let $C(m,q) = \mathcal{C}_{m,q}$ be an Hermitian code. So

$$z \in \mathcal{C}_{m,q} \iff z\mathbf{H} = 0$$
$$\sum_{i=1}^{n} z_i f_j(P_i) = 0 \quad \forall j = 1, \ldots, n-k \text{ for } f_j \in \mathcal{B}_{m,q} = \{f_1, \ldots, f_{n-k}\}$$

All words of weight w correspond to solutions of this system:

$$J_{q,m}(w) = \begin{cases} \sum_{i=1}^{w} z_i x_i^r y_i^s = 0 \quad \forall\, r,s \quad \text{for} \quad x^r y^s \in \mathcal{B}_{m,q} \\ x_i^{q+1} - y_i^q - y_i = 0 \quad \forall\, i = 1, \ldots, w \\ x_i^{q^2} - x_i = 0 \quad y_i^{q^2} - y_i = 0 \quad z_i^{q^2-1} - 1 = 0 \quad \forall\, i = 1, \ldots, w \\ \prod_{1 \le i < j \le w} ((x_i - x_j)^{q^2-1} - 1)((y_i - y_j)^{q^2-1} - 1) = 0 \end{cases}$$

$$A_w(\mathcal{C}_{m,q}(w)) = \frac{|\mathcal{V}(J_{q,m}(w))|}{w!}$$

The number of codewords

Let $C(m,q) = \mathcal{C}_{m,q}$ be an Hermitian code. So

$$z \in \mathcal{C}_{m,q} \iff z\mathbf{H} = 0$$
$$\sum_{i=1}^{n} z_i f_j(P_i) = 0 \quad \forall j = 1, \ldots, n-k \text{ for } f_j \in \mathcal{B}_{m,q} = \{f_1, \ldots, f_{n-k}\}$$

All words of weight w correspond to solutions of this system:

$$J_{q,m}(w) = \begin{cases} \sum_{i=1}^{w} z_i x_i^r y_i^s = 0 \quad \forall\, r,s \quad \text{for} \quad x^r y^s \in \mathcal{B}_{m,q} \\ x_i^{q+1} - y_i^q - y_i = 0 \quad \forall\, i = 1, \ldots, w \\ x_i^{q^2} - x_i = 0 \quad y_i^{q^2} - y_i = 0 \quad z_i^{q^2-1} - 1 = 0 \quad \forall\, i = 1, \ldots, w \\ \prod_{1 \le i < j \le w} ((x_i - x_j)^{q^2-1} - 1)((y_i - y_j)^{q^2-1} - 1) = 0 \end{cases}$$

$$A_w(\mathcal{C}_{m,q}(w)) = \frac{|\mathcal{V}(J_{q,m}(w))|}{w!}$$

The number of codewords

Let $C(m,q)=\mathcal{C}_{m,q}$ be an Hermitian code. So

$$z\in\mathcal{C}_{m,q} \iff z\mathbf{H}=0$$
$$\sum_{i=1}^{n} z_i f_j(P_i)=0 \quad \forall j=1,\dots,n-k \text{ for } f_j\in\mathcal{B}_{m,q}=\{f_1,\dots,f_{n-k}\}$$

All words of weight w correspond to solutions of this system:

$$J_{q,m}(w)=\begin{cases} \sum_{i=1}^{w} z_i x_i^r y_i^s=0 \quad \forall\, r,s \quad \text{for} \quad x^r y^s\in\mathcal{B}_{m,q} \\ x_i^{q+1}-y_i^q-y_i=0 \quad \forall\, i=1,\dots,w \\ x_i^{q^2}-x_i=0 \quad y_i^{q^2}-y_i=0 \quad z_i^{q^2-1}-1=0 \quad \forall\, i=1,\dots,w \\ \prod_{1\le i<j\le w}((x_i-x_j)^{q^2-1}-1)((y_i-y_j)^{q^2-1}-1)=0 \end{cases}$$

$$A_w(\mathcal{C}_{m,q}(w))=\frac{|\mathcal{V}(J_{q,m}(w))|}{w!}$$

Minimum weight codewords for some Hermitian codes

Edge Code

Theorem

The minimum weight words of an Edge Code H_d^j are

$$A_d = q^2(q^2-1)\binom{q}{d}$$

We use this lemma

Lemma

The minimum weight words correspond to points lying on a vertical line.

Edge Code

Theorem

The minimum weight words of an Edge Code H_d^j are

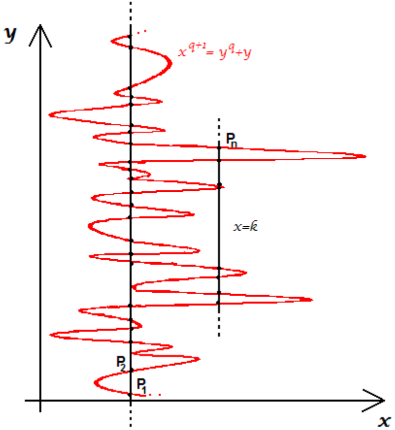
$$A_d = q^2(q^2 - 1)\binom{q}{d}$$

We use this lemma

Lemma

The minimum weight words correspond to points lying on a vertical line.

Sketch of proof



Let $x, y \in \mathbb{F}_{q^2}$

$$\begin{cases} x^{q+1} = y^q + y \\ x = k \end{cases}$$

We have to solve this equation

$$t = k^{q+1} = y^q + y$$

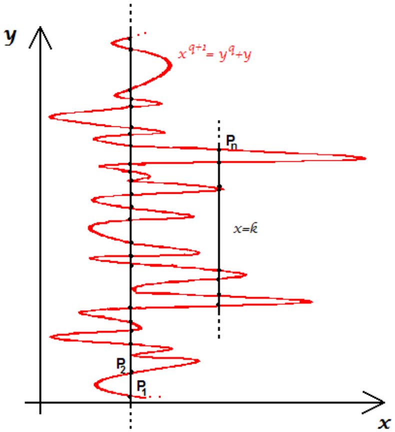
So

$$q^2 \quad \binom{q}{d} \quad \#z$$

$$\downarrow \qquad \downarrow$$

$$x \qquad y$$

Sketch of proof



Let $x, y \in \mathbb{F}_{q^2}$

$$\begin{cases} x^{q+1} = y^q + y \\ x = k \end{cases}$$

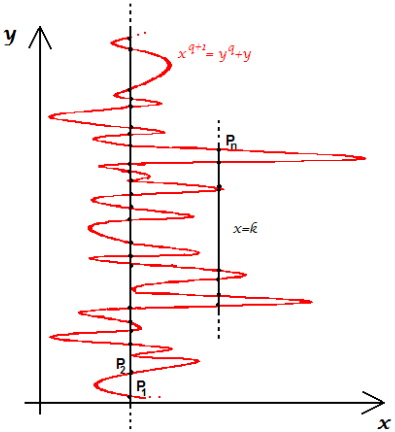
We have to solve this equation

$$t = k^{q+1} = y^q + y$$

So

$$\begin{matrix} q^2 & \binom{q}{d} & \#z \\ \downarrow & \downarrow & \\ x & y & \end{matrix}$$

Sketch of proof



Let $x, y \in \mathbb{F}_{q^2}$

$$\begin{cases} x^{q+1} = y^q + y \\ x = k \end{cases}$$

We have to solve this equation

$$t = k^{q+1} = y^q + y$$

So

$$\begin{array}{ccc} q^2 & \binom{q}{d} & \#z \\ \downarrow & \downarrow & \\ x & y & \end{array}$$

Sketch of proof

We know that $\sum_{i=1}^{d} z_i x_i^r y_i^s = 0$ where $x^r y^s \in \mathcal{B}_{m,q}$. Then

$$\begin{cases} z_1 + \cdots + z_d = 0 \\ y_1 z_1 + \cdots + y_d z_d = 0 \\ \quad \vdots \\ y_1^{d-2} z_1 + \cdots + y_d^{d-2} z_d = 0 \end{cases}$$

The solutions in z are

$$(a_1\alpha, a_2\alpha, \ldots, a_{d-1}\alpha, \alpha) \quad \text{with} \quad \alpha \in \mathbb{F}_{q^2}^*.$$

For this reason

$$\#z = q^2 - 1.$$

Sketch of proof

We know that $\sum_{i=1}^{d} z_i x_i^r y_i^s = 0$ where $x^r y^s \in \mathcal{B}_{m,q}$. Then

$$\begin{cases} z_1 + \cdots + z_d = 0 \\ y_1 z_1 + \cdots + y_d z_d = 0 \\ \quad \vdots \\ y_1^{d-2} z_1 + \cdots + y_d^{d-2} z_d = 0 \end{cases}$$

The solutions in z are

$$(a_1\alpha, a_2\alpha, \ldots, a_{d-1}\alpha, \alpha) \quad \text{with} \quad \alpha \in \mathbb{F}_{q^2}^*.$$

For this reason

$$\#z = q^2 - 1.$$

Sketch of proof

We know that $\sum_{i=1}^{d} z_i x_i^r y_i^s = 0$ where $x^r y^s \in \mathcal{B}_{m,q}$. Then

$$\begin{cases} z_1 + \cdots + z_d = 0 \\ y_1 z_1 + \cdots + y_d z_d = 0 \\ \quad \vdots \\ y_1^{d-2} z_1 + \cdots + y_d^{d-2} z_d = 0 \end{cases}$$

The solutions in z are

$$(a_1\alpha, a_2\alpha, \ldots, a_{d-1}\alpha, \alpha) \quad \text{with} \quad \alpha \in \mathbb{F}_{q^2}^*.$$

For this reason

$$\#z = q^2 - 1.$$

Sketch of proof

We know that $\sum_{i=1}^{d} z_i x_i^r y_i^s = 0$ where $x^r y^s \in \mathcal{B}_{m,q}$. Then

$$\begin{cases} z_1 + \cdots + z_d = 0 \\ y_1 z_1 + \cdots + y_d z_d = 0 \\ \quad \vdots \\ y_1^{d-2} z_1 + \cdots + y_d^{d-2} z_d = 0 \end{cases}$$

The solutions in z are

$$(a_1\alpha, a_2\alpha, \ldots, a_{d-1}\alpha, \alpha) \quad \text{with} \quad \alpha \in \mathbb{F}_{q^2}^*.$$

For this reason

$$\#z = q^2 - 1.$$

Corner Codes

Theorem

The minimum weight words of a Corner Code H_d^0 are

$$A_d = q^2(q^2-1)\binom{q}{d-1}\frac{q^3-d+1}{d}$$

To prove the theorem we use this

Lemma

The words of minimum weight are the points lying in the intersection of any line and the curve.

Corner Codes

Theorem

The minimum weight words of a Corner Code H_d^0 are

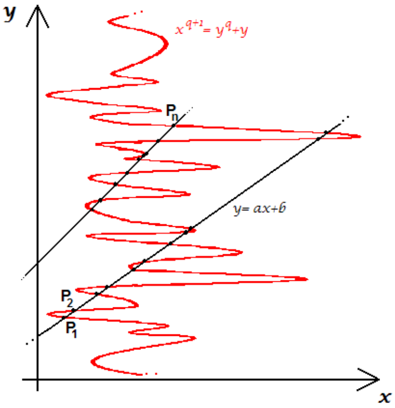
$$A_d = q^2(q^2-1)\binom{q}{d-1}\frac{q^3-d+1}{d}$$

To prove the theorem we use this

Lemma

The words of minimum weight are the points lying in the intersection of any line and the curve.

Sketch of proof



Let $x, y \in \mathbb{F}_{q^2}$

$$\begin{cases} x^{q+1} = y^q + y \\ y = ax + b \end{cases}$$

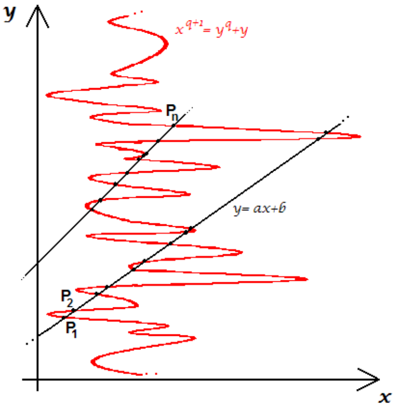
If we solve the system we find

$$a^q x^q + b^q + ax + b = x^{q+1}$$

So

$$\underset{y}{\underset{\downarrow}{(q^4 - q^3)}} \quad \underset{x}{\underset{\downarrow}{\binom{q+1}{d}}} \quad \underset{z}{\underset{\downarrow}{(q^2 - 1)}}$$

Sketch of proof



Let $x, y \in \mathbb{F}_{q^2}$

$$\begin{cases} x^{q+1} = y^q + y \\ y = ax + b \end{cases}$$

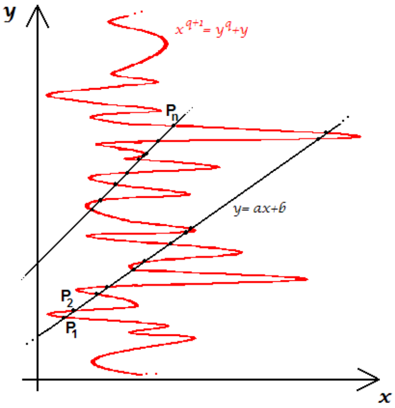
If we solve the system we find

$$a^q x^q + b^q + ax + b = x^{q+1}$$

So

$$(q^4 - q^3) \quad \binom{q+1}{d} \quad (q^2 - 1)$$
$$\downarrow \qquad \downarrow \qquad \downarrow$$
$$y \qquad x \qquad z$$

Sketch of proof



Let $x, y \in \mathbb{F}_{q^2}$

$$\begin{cases} x^{q+1} = y^q + y \\ y = ax + b \end{cases}$$

If we solve the system we find

$$a^q x^q + b^q + ax + b = x^{q+1}$$

So

$$\begin{array}{ccc} (q^4 - q^3) & \binom{q+1}{d} & (q^2 - 1) \\ \downarrow & \downarrow & \downarrow \\ y & x & z \end{array}$$

Sketch of proof

The number of points corresponding to a vertical line is

$$q^2(q^2-1)\binom{q}{d}$$

whereas those corresponding to non-vertical lines are:

$$(q^4-q^3)\binom{q+1}{d}(q^2-1)$$

So to find the result of the theorem we have to sum these two values.

Sketch of proof

The number of points corresponding to a vertical line is

$$q^2(q^2-1)\binom{q}{d}$$

whereas those corresponding to non-vertical lines are:

$$(q^4-q^3)\binom{q+1}{d}(q^2-1)$$

So to find the result of the theorem we have to sum these two values.

Sketch of proof

The number of points corresponding to a vertical line is

$$q^2(q^2-1)\binom{q}{d}$$

whereas those corresponding to non-vertical lines are:

$$(q^4-q^3)\binom{q+1}{d}(q^2-1)$$

So to find the result of the theorem we have to sum these two values.

The small weight words of some Hermitian codes

The case with $y_1 = \cdots = y_{d+1}$

Theorem (Corner Code)

The number of words of weight $d+1$ with $y_1 = \cdots = y_{d+1}$ of a Corner Code H_d^0 is:

$$A_{d+1} = \frac{(q^2-q)(q^4-(d+1)q^2+d)}{(d+1)!}\binom{q+1}{d+1}$$

Theorem (Edge Code)

The words of weight $d+1$ with $y_1 = \cdots = y_{d+1}$ of an Edge Code H_d^j with $1 \leq j \leq d-1$ are:

$$A_{d+1} = \frac{(q^2-1)(q^2-q)}{(d+1)!}\binom{q+1}{d+1}$$

The case with $y_1 = \cdots = y_{d+1}$

Theorem (Corner Code)

The number of words of weight $d+1$ with $y_1 = \cdots = y_{d+1}$ of a Corner Code H_d^0 is:

$$A_{d+1} = \frac{(q^2-q)(q^4-(d+1)q^2+d)}{(d+1)!}\binom{q+1}{d+1}$$

Theorem (Edge Code)

The words of weight $d+1$ with $y_1 = \cdots = y_{d+1}$ of an Edge Code H_d^j with $1 \leq j \leq d-1$ are:

$$A_{d+1} = \frac{(q^2-1)(q^2-q)}{(d+1)!}\binom{q+1}{d+1}$$

Sketch of proof for $y_1 = \ldots = y_{d+1}$

The points (x_i, y_i) lie on the Hermitian curve $x_i^{q+1} = y_i^q + y_i$.

$$\#y = q^2 - q \quad \text{and} \quad \#x = \binom{q+1}{d+1}$$

The z's have to verify $\sum_{i=1}^{d} z_i x_i^r y_i^s = 0$ where $x^r y^s \in \mathcal{B}_{m,q}$.

Corner Code

$$\begin{cases} z_1 + \cdots + z_{d+1} = 0 \\ x_1 z_1 + \cdots + x_{d+1} z_{d+1} = 0 \\ x_1^2 z_1 + \cdots + x_{d+1}^2 z_{d+1} = 0 \\ \quad \vdots \\ x_1^{d-2} z_1 + \cdots + x_{d+1}^{d-2} z_{d+1} = 0 \end{cases}$$

Sketch of proof for $y_1 = \ldots = y_{d+1}$

The points (x_i, y_i) lie on the Hermitian curve $x_i^{q+1} = y_i^q + y_i$.

$$\#y = q^2 - q \quad \text{and} \quad \#x = \binom{q+1}{d+1}$$

The z's have to verify $\sum_{i=1}^{d} z_i x_i^r y_i^s = 0$ where $x^r y^s \in \mathcal{B}_{m,q}$.

Corner Code

$$\begin{cases} z_1 + \cdots + z_{d+1} = 0 \\ x_1 z_1 + \cdots + x_{d+1} z_{d+1} = 0 \\ x_1^2 z_1 + \cdots + x_{d+1}^2 z_{d+1} = 0 \\ \quad \vdots \\ x_1^{d-2} z_1 + \cdots + x_{d+1}^{d-2} z_{d+1} = 0 \end{cases}$$

Sketch of proof for $y_1 = \ldots = y_{d+1}$

The points (x_i, y_i) lie on the Hermitian curve $x_i^{q+1} = y_i^q + y_i$.

$$\#y = q^2 - q \quad \text{and} \quad \#x = \binom{q+1}{d+1}$$

The z's have to verify $\sum_{i=1}^{d} z_i x_i^r y_i^s = 0$ where $x^r y^s \in \mathcal{B}_{m,q}$.

Corner Code

$$\begin{cases} z_1 + \cdots + z_{d+1} = 0 \\ x_1 z_1 + \cdots + x_{d+1} z_{d+1} = 0 \\ x_1^2 z_1 + \cdots + x_{d+1}^2 z_{d+1} = 0 \\ \quad \vdots \\ x_1^{d-2} z_1 + \cdots + x_{d+1}^{d-2} z_{d+1} = 0 \end{cases}$$

Sketch of proof for $y_1 = \ldots = y_{d+1}$

The points (x_i, y_i) lie on the Hermitian curve $x_i^{q+1} = y_i^q + y_i$.

$$\#y = q^2 - q \quad \text{and} \quad \#x = \binom{q+1}{d+1}$$

The z's have to verify $\sum_{i=1}^{d} z_i x_i^r y_i^s = 0$ where $x^r y^s \in \mathcal{B}_{m,q}$.

Corner Code

$$\begin{cases} z_1 + \cdots + z_{d+1} = 0 \\ x_1 z_1 + \cdots + x_{d+1} z_{d+1} = 0 \\ x_1^2 z_1 + \cdots + x_{d+1}^2 z_{d+1} = 0 \\ \quad \vdots \\ x_1^{d-2} z_1 + \cdots + x_{d+1}^{d-2} z_{d+1} = 0 \end{cases}$$

$$\Downarrow$$

$$\#z = q^2 \cdot q^2 - \#(z_i = 0 \text{ for some } i)$$

$$\#z = q^4 - (d+1)q + d$$

Sketch of proof for $y_1 = \ldots = y_{d+1}$

The points (x_i, y_i) lie on the Hermitian curve $x_i^{q+1} = y_i^q + y_i$.

$$\#y = q^2 - q \quad \text{and} \quad \#x = \binom{q+1}{d+1}$$

The z's have to verify $\sum_{i=1}^{d} z_i x_i^r y_i^s = 0$ where $x^r y^s \in \mathcal{B}_{m,q}$.

Corner Code

$$\begin{cases} z_1 + \cdots + z_{d+1} = 0 \\ x_1 z_1 + \cdots + x_{d+1} z_{d+1} = 0 \\ x_1^2 z_1 + \cdots + x_{d+1}^2 z_{d+1} = 0 \\ \quad \vdots \\ x_1^{d-2} z_1 + \cdots + x_{d+1}^{d-2} z_{d+1} = 0 \end{cases}$$

$$\Downarrow$$

$$\#z = q^4 - (d+1)q + d$$

Edge Code

$$\begin{cases} z_1 + \cdots + z_{d+1} = 0 \\ x_1 z_1 + \cdots + x_{d+1} z_{d+1} = 0 \\ x_1^2 z_1 + \cdots + x_{d+1}^2 z_{d+1} = 0 \\ \quad \vdots \\ x_1^{d-1} z_1 + \cdots + x_{d+1}^{d-1} z_{d+1} = 0 \end{cases}$$

$$\Downarrow$$

$$\#z = q^2 - 1$$

The case with $x_1 = \cdots = x_{d+1}$

Theorem (Corner Code)

The number of words of weight $d+1$ with $x_1 = \cdots = x_{d+1}$ of a Corner Code H_d^0 is:

$$A_{d+1} = \frac{q^2(q^4 - (d+1)q^2 + d)}{(d+1)!} \binom{q}{d+1}$$

Theorem (Edge Code)

The words of weight $d+1$ with $x_1 = \cdots = x_{d+1}$ of an Edge Code H_d^j are:

$$A_{d+1} = \frac{q^2(q^2 - 1)}{(d+1)!} \binom{q}{d+1}$$

The case with $x_1 = \cdots = x_{d+1}$

Theorem (Corner Code)

The number of words of weight $d+1$ with $x_1 = \cdots = x_{d+1}$ of a Corner Code H_d^0 is:

$$A_{d+1} = \frac{q^2(q^4 - (d+1)q^2 + d)}{(d+1)!} \binom{q}{d+1}$$

Theorem (Edge Code)

The words of weight $d+1$ with $x_1 = \cdots = x_{d+1}$ of an Edge Code H_d^j are:

$$A_{d+1} = \frac{q^2(q^2 - 1)}{(d+1)!} \binom{q}{d+1}$$

Sketch of proof for $x_1 = \ldots = x_{d+1}$

The points (x_i, y_i) lie on the Hermitian curve $x_i^{q+1} = y_i^q + y_i$.

$$\#x = q^2 \quad \text{and} \quad \#y = \binom{q}{d+1}$$

The z's have to verify $\sum_{i=1}^{d} z_i x_i^r y_i^s = 0$ where $x^r y^s \in \mathcal{B}_{m,q}$.

Corner Code

$$\begin{cases} z_1 + \cdots + z_{d+1} = 0 \\ x_1 z_1 + \cdots + x_{d+1} z_{d+1} = 0 \\ x_1^2 z_1 + \cdots + x_{d+1}^2 z_{d+1} = 0 \\ \quad \vdots \\ x_1^{d-2} z_1 + \cdots + x_{d+1}^{d-2} z_{d+1} = 0 \end{cases}$$

Sketch of proof for $x_1 = \ldots = x_{d+1}$

The points (x_i, y_i) lie on the Hermitian curve $x_i^{q+1} = y_i^q + y_i$.

$$\#x = q^2 \quad \text{and} \quad \#y = \binom{q}{d+1}$$

The z's have to verify $\sum_{i=1}^{d} z_i x_i^r y_i^s = 0$ where $x^r y^s \in \mathcal{B}_{m,q}$.

Corner Code

$$\begin{cases} z_1 + \cdots + z_{d+1} = 0 \\ x_1 z_1 + \cdots + x_{d+1} z_{d+1} = 0 \\ x_1^2 z_1 + \cdots + x_{d+1}^2 z_{d+1} = 0 \\ \quad \vdots \\ x_1^{d-2} z_1 + \cdots + x_{d+1}^{d-2} z_{d+1} = 0 \end{cases}$$

Sketch of proof for $x_1 = \ldots = x_{d+1}$

The points (x_i, y_i) lie on the Hermitian curve $x_i^{q+1} = y_i^q + y_i$.

$$\#x = q^2 \quad \text{and} \quad \#y = \binom{q}{d+1}$$

The z's have to verify $\sum_{i=1}^{d} z_i x_i^r y_i^s = 0$ where $x^r y^s \in \mathcal{B}_{m,q}$.

Corner Code

$$\begin{cases} z_1 + \cdots + z_{d+1} = 0 \\ x_1 z_1 + \cdots + x_{d+1} z_{d+1} = 0 \\ x_1^2 z_1 + \cdots + x_{d+1}^2 z_{d+1} = 0 \\ \quad \vdots \\ x_1^{d-2} z_1 + \cdots + x_{d+1}^{d-2} z_{d+1} = 0 \end{cases}$$

Sketch of proof for $x_1 = \ldots = x_{d+1}$

The points (x_i, y_i) lie on the Hermitian curve $x_i^{q+1} = y_i^q + y_i$.

$$\#x = q^2 \quad \text{and} \quad \#y = \binom{q}{d+1}$$

The z's have to verify $\sum_{i=1}^{d} z_i x_i^r y_i^s = 0$ where $x^r y^s \in \mathcal{B}_{m,q}$.

Corner Code

$$\begin{cases} z_1 + \cdots + z_{d+1} = 0 \\ x_1 z_1 + \cdots + x_{d+1} z_{d+1} = 0 \\ x_1^2 z_1 + \cdots + x_{d+1}^2 z_{d+1} = 0 \\ \quad \vdots \\ x_1^{d-2} z_1 + \cdots + x_{d+1}^{d-2} z_{d+1} = 0 \end{cases}$$

$$\Downarrow$$

$$\#z = q^4 - (d+1)q + d$$

Sketch of proof for $x_1 = \ldots = x_{d+1}$

The points (x_i, y_i) lie on the Hermitian curve $x_i^{q+1} = y_i^q + y_i$.

$$\#x = q^2 \quad \text{and} \quad \#y = \binom{q}{d+1}$$

The z's have to verify $\sum_{i=1}^{d} z_i x_i^r y_i^s = 0$ where $x^r y^s \in \mathcal{B}_{m,q}$.

Corner Code

$$\begin{cases} z_1 + \cdots + z_{d+1} = 0 \\ x_1 z_1 + \cdots + x_{d+1} z_{d+1} = 0 \\ x_1^2 z_1 + \cdots + x_{d+1}^2 z_{d+1} = 0 \\ \vdots \\ x_1^{d-2} z_1 + \cdots + x_{d+1}^{d-2} z_{d+1} = 0 \end{cases}$$

$$\Downarrow$$

$$\#z = q^4 - (d+1)q + d$$

Edge Code

$$\begin{cases} z_1 + \cdots + z_{d+1} = 0 \\ x_1 z_1 + \cdots + x_{d+1} z_{d+1} = 0 \\ x_1^2 z_1 + \cdots + x_{d+1}^2 z_{d+1} = 0 \\ \vdots \\ x_1^{d-1} z_1 + \cdots + x_{d+1}^{d-1} z_{d+1} = 0 \end{cases}$$

$$\Downarrow$$

$$\#z = q^2 - 1$$

The number of codewords of H_3^0

Coordinates of points | **H_3^0**

$x_i \neq x_j$	$y_i = y_j$	$\frac{1}{24}(q^4 - 4q^2 + 3)(q^2 - q)\binom{q+1}{4}$
	$y_1 = y_2 = y_3 \neq y_4$	0
	$y_1 = y_2 \neq y_3 = y_4$	$\frac{1}{8}q^2(q^2-1)^2(q-2)(q^3+2q^2-2q+1)$
	$y_1 = y_2 \neq y_3, y_4$ $y_3 \neq y_4$	$A_4 > \frac{1}{4}q^2(q^2-1)^2(2q^6-7q^5-6q^4+19q^3-9q^2-4q+4)$ $A_4 < \frac{1}{4}q^2(q^2-1)^2(2q^6-3q^5-11q^4+9q^3+25q^2-14q+4)$
	$y_i \neq y_j$	?
$x_i = x_j$	$y_i \neq y_j$	$\frac{1}{24}q^2(q^4-4q^2+3)\binom{q}{4}$

Thank you for your attention!