On the weights of affine-variety codes and some Hermitian codes

Marco Pellegrini

University of Pisa, Italy
Department of Mathematics

Trento, 12 settembre 2011

Summary

Introduction

For any affine-variety code we show that we can construct an ideal whose solutions correspond to codewords with any assigned weight. We use our ideal and a geometric characterization to determine the number of small-weight codewords for some families of Hermitian codes over any $\mathbb{F}_{q^2}$. In particular, we determine the number of minimum-weight codewords for all Hermitian codes with $d \leq q$. For such codes we also count some other small-weight codewords.

Acknowledgements

This work is jointly with Chiara Marcolla and our supervisor Massimiliano Sala.

Hermitian curve

We consider the Hermitian curve $\mathcal{H}$ 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

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

This curve has exactly $n = q^3$ rational points,
that we call $\mathcal{P} = \{P_1, \ldots, P_n\}$.

Hermitian code

Definition

The evaluation map is

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

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

Let m a natural number, then we define

$$\mathcal{B}_{q,m} = \{x^r y^s | qr + (q+1)s \leq m, 0 \leq s \leq q-1\}$$

So we consider

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

Hermitian code

Therefore

$$C_m = (E_m)^{\perp} = \{c \in (\mathbb{F}_{q^2})^n | c \cdot ev_{\mathcal{P}}(f) = 0, f \in \mathcal{B}_{q,m}\}$$

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

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

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

The number of codewords

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

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

If we write $\mathcal{B}_{q,m} = \{f_1, \ldots, f_{n-k}\}$, then

$$\sum_{i=1}^{n} f_j(P_i) z_i = 0 \qquad \forall j = 1, \ldots, n-k$$

The number of codewords

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

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

The number of codewords of weight w is

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

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	$q^3 \leq m \leq q^3 + q^2 - q - 2$

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

Corner code

If H is composed of the evaluation of these sets

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

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

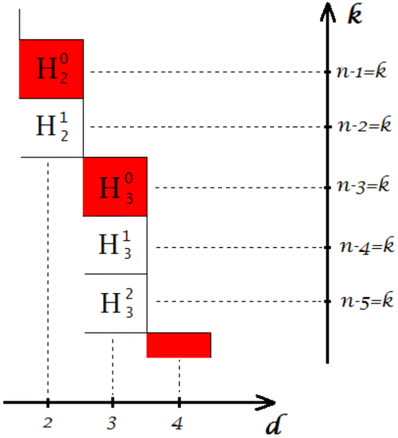
The code having parity-check matrix composed of $L_0^d \cup \ldots \cup L_{d-2}^d$ and of

$$\begin{array}{l} l_1^d = x^{d-1} \\ l_2^d = x^{d-2}y \\ \quad\quad \vdots \\ l_j^d = x^{d-j}y^{j-1} \end{array}$$

is called an edge code, indicated 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 and edge code



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

v-block position

Let $w \geq v \geq 1$. Let
$Q = (x_1, \ldots, x_w, y_1, \ldots, y_w, z_1, \ldots, z_w) \in \mathcal{V}(J_{q,m,w})$, then Q is in v-block position if we can partition $\{1, \ldots, n\}$ in v blocks $I_1, \ldots, I_v$ such that

$$x_i = x_j \iff \exists h \text{ such that } 1 \leq h \leq v \text{ and } i, j \in I_h$$

We can assume $|I_1| \leq \ldots \leq |I_v|$ and $I_1 = \{1, \ldots, u\}$.

Lemma

We always have $u + v \leq w + 1$. If $u \geq 2$ and $v \geq 2$, then $v \leq \lfloor \frac{w}{2} \rfloor$ and $u + v \leq \lfloor \frac{w}{2} \rfloor + 2$.

Edge code

Lemma

Let H_d^j be an edge code with $1 \leq j \leq d-1$ and $3 \leq d \leq w \leq 2d-3$. Let $Q = (x_1, \dots, x_w, y_1, \dots, y_w, z_1, \dots, z_w) \in \mathcal{V}(J_{q,m,w})$ in v-block position, with $v \leq w$, then either

(a) $u = 1$ and $v > d$ and $w \geq d+1$, or

(b) $v = 1$, that is, $x_1 = \cdots = x_w$

We have the following corollary:

Corollary

The minimum weight words correspond to points of $\mathcal{H}$ lying on a vertical line.

Sketch of proof (a)

We denote for all h such that $1 \leq h \leq v$

$$X_h = x_i \text{ if } i \in I_h, \quad Z_h = \sum_{i \in I_h} z_i, \quad Y_{h,s} = \sum_{i \in I_h} y_i^s z_i,$$

with $1 \leq s \leq u-1$. Let $v \leq d$. We know that $\sum_{i=1}^{w} x_i^r z_i = \sum_{h=1}^{v} X_h^r Z_h$, where $0 \leq r \leq d-1$. We can consider the first v equations

$$\begin{pmatrix} 1 & \cdots & 1 \\ X_1 & \cdots & X_v \\ \vdots & \ddots & \vdots \\ X_1^{v-1} & \cdots & X_v^{v-1} \end{pmatrix} \begin{pmatrix} Z_1 \\ \vdots \\ Z_v \end{pmatrix} = 0$$

The solution of the previous system is $Z_h = 0$ for any h. Since $u = 1$, then $Z_1 = z_1 = 0$, which is impossible. So $v > d$, then $w \geq d+1$.

Sketch of proof (b)

Let $u \geq 2$. Suppose that $v \geq 2$. We know that $\sum_{i=1}^{w} x_i^r y_i^s z_i = 0$ where $x^r y^s \in \mathcal{B}_{q,m}$. Then a subset is

$$\left\{\begin{array}{l} \sum_{i=1}^{w} x_i^r z_i = 0 \\ \sum_{i=1}^{w} x_i^r y_i z_i = 0 \\ \qquad \vdots \\ \sum_{i=1}^{w} x_i^r y_i^{u-1} z_i = 0 \end{array}\right. \iff \left\{\begin{array}{l} \sum_{h=1}^{v} X_h^r Z_h = 0 \\ \sum_{h=1}^{v} X_h^r Y_{h,1} = 0 \\ \qquad \vdots \\ \sum_{h=1}^{v} X_h^r Y_{h,u-1} = 0 \end{array}\right.$$

where $0 \leq r \leq v$. This implies that $Z_1 = Y_{1,1} = \ldots = Y_{1,u-1} = 0$, that is

$$\left\{\begin{array}{l} \sum_{i=1}^{u} z_i = 0 \\ \sum_{i=1}^{u} y_i z_i = 0 \\ \qquad \vdots \\ \sum_{i=1}^{u} y_i^{u-1} z_i = 0 \end{array}\right. \implies z_1 = \cdots = z_u = 0.$$

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 the previous corollary: the minimum weight words correspond to points of $\mathcal{H}$ lying on a vertical line.

Sketch of proof

For any $x \in \mathbb{F}_{q^2}$, the equation $x^{q+1} = y^q + y$ has exactly q solutions. We have q^2 ways to choose x, $\binom{q}{d}$ ways to choose d points of $\mathcal{H}$ on a vertical line. The system $J_{q,m,w}$ becomes

$$\begin{cases} \sum_{i=1}^{d} z_i = 0 \\ \sum_{i=1}^{d} y_i z_i = 0 \\ \qquad \vdots \\ \sum_{i=1}^{d} y_i^{d-2} z_i = 0 \end{cases}$$

The solutions in z_i are of the form $(a_1\alpha, \ldots, a_d\alpha)$, for any $\alpha \in \mathbb{F}_{q^2}^*$. For this reason, we have $q^2 - 1$ solutions in z_i.

Corner code

Proposition

The minimum weight words of a corner code H_d^0 correspond to points lying in the intersection of any line and the curve $\mathcal{H}$.

Sketch of proof

From system $J_{q,m,w}$ we can deduce

$$\begin{cases} \sum_{i=1}^{d} z_i = 0 \\ \sum_{i=1}^{d} x_i z_i = 0 \\ \qquad \vdots \\ \sum_{i=1}^{d} x_i^{d-2} z_i = 0 \end{cases}$$

and we know that the z_i are all non-zero if x_i are all distinct or all equal. For the same reason, we can also deduce that y_i are all distinct or all equal.

Sketch of proof

If the x_i are all equal or the y_i are all equal, we have finished. Otherwise, we do an affine transformation

$$\begin{cases} x = x' \\ y = y' + ax' \end{cases} \qquad a \in \mathbb{F}_{q^2}$$

such that at least two y_i are equal. Substituting the above transformation into the system $J_{q,m,w}$ and making elementary row operations we get once again the system $J_{q,m,w}$. But, since at least two y_i are equal, they are all equal.

Corner code

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 the previous proposition: the minimum weight words correspond to points lying in the intersection of any line and the curve $\mathcal{H}$.

Sketch of proof

We have to solve the system

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

from which we have $a^q x^q + b^q + ax + b = x^{q+1}$. If $b^q + b + a^{q+1} = 0$, the equation becomes $(x - a^q)^{q+1} = 0$, so we have only one point; there are exactly q^3 such possibilities for (a, b).
If $b^q + b + a^{q+1} = c \neq 0$, we have that $c \in \mathbb{F}_q$, the equation becomes $(x - a^q)^{q+1} = (\alpha^r)^{q+1}$, where α is a primitive element of $\mathbb{F}_{q^2}$ and r is an integer, so that we have exactly $q + 1$ solutions.
So, we have $(q^4 - q^3)$ ways to choose a line $y = ax + b$, $\binom{q+1}{d}$ ways to choose d points on it, $q^2 - 1$ solutions in z_i.

Sketch of proof

The number of words corresponding to points on a vertical line is

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

whereas those corresponding to non-vertical lines are:

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

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

The second weight

The problem of finding the number of codewords of weight $d+1$ for a first-phase hermitian code, where d is the distance, is more complicated.
In fact, we can not say in general that such codewords correspond to points on a same line.
Nevertheless, we can count codewords that have this property. By similar arguments, we can state the following theorems.

The case of vertical lines

Theorem (corner code and edge code)

The number of words of weight $d+1$ with $x_1 = \cdots = x_{d+1}$ of a corner code H_d^0 and of an edge code H_d^j is:

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

The case of non-vertical lines

Theorem (corner code)

The number of words of weight $d+1$ of a corner code H_d^0 with (x_i, y_i) lying on a non-vertical line is:

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

Theorem (edge code)

The number of words of weight $d+1$ of an edge code H_d^j with (x_i, y_i) lying on a non-vertical line is:

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

The case of H_3^0

To count the number of words with weight $w = 4$, we observed that:

- in system $J_{q,m,4}$ we can have 4 points on a same line;
- we can not have 3 points on a same line and the other outside;
- we can have 4 points in general position, that is, no 3 of them lie on a same line.

So finally we have

$$A_4 = \left(\binom{q^3}{4} - q^2 \binom{q}{3} (q^3 - q) - (q^4 - q^3) \binom{q+1}{3} (q^3 - q - 1) \right) (q^2 - 1) +$$

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

The case of H_3^1

To count the number of words with weight $w = 4$, we observed that:

- in system $J_{q,m,4}$ we can have 4 points on a same line;
- we can not have 3 points on a same line and the other outside;
- we can have 2 points on a vertical line and 2 on another one;
- we can have 4 points on a same parabola of the form $y = ax^2 + bx + c$.

So finally we have

$$A_4 = q^2 \binom{q}{4}(q^4 - 4q^2 + 3) + \frac{q^4(q^2-1)^2(q-1)^2}{8} + (q^2-1)\sum_{k=4}^{2q} N_k \binom{k}{4}$$

where N_k is the number of parabolas that intersect $\mathcal{H}$ in exactly k points.

Other cases

We also studied codes H_3^2 (with $w = 4$), H_4^0 and H_4^1 (with $w = 5$).
In general, we have to study the rank of the matrix

$$H' = \begin{pmatrix} 1 & \cdots & 1 \\ x_1 & \cdots & x_w \\ \vdots & \ddots & \vdots \\ x_1^r y_1^s & \cdots & x_w^r y_w^s \\ \cdots & \cdots & \cdots \end{pmatrix}$$

for any choice of w points (x_i, y_i) of $\mathcal{H}$.
For these three codes, we have that all codewords of weight $d + 1$ correspond to points on a same line (so that we can apply the previous theorems).

Work in progress

- We believe that many of these ideas can be applied to other affine-variety codes.
- We are trying to find the number of parabolas that intersect $\mathcal{H}$ in exactly k points.
- By computer elaborations we see that, if we write the list of A_d for every Hermitian code in phase three, ordered by dimension, then that list is symmetric.
- We are trying to see if, for codewords of minimum weight in every phase, they always correspond to points grouped in lines or conics.