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

Marco Pellegrini, Chiara Marcolla, Massimiliano Sala

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

Marco Pellegrini[1], Chiara Marcolla[2], and Massimiliano Sala[3]

[1] Department of Mathematics, University of Pisa, Italy
pellegrini@mail.dm.unipi.it
[2] Department of Mathematics, University of Trento, Italy
chiara.marcolla@unitn.it
[3] maxsalacodes@gmail.com

Abstract. For any affine-variety code we show how to 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 $\mathbb{F}_q$. 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.

Keywords: Affine-variety codes, linear code, distance, minimum-weight word, Hermitian code.

1 Preliminary results

Let $\mathbb{F}_q$ be a finite field. Let $k \geq 1$. For any ideal I in a polynomial ring $\mathbb{F}_q[X]$, where $X = \{x_1, \ldots, x_k\}$, we denote by $\mathcal{V}(I) \subset (\overline{\mathbb{F}}_q)^k$ its variety. For any $Z \subset (\overline{\mathbb{F}}_q)^k$ we denote by $\mathcal{I}(Z) \subset \mathbb{F}_q[X]$ the vanishing ideal of Z.

Let $g_1, \ldots, g_s \in \mathbb{F}_q[X]$, we denote by $I = \langle g_1, \ldots, g_s \rangle$ the ideal generated by the g_i's. Let $\{x_1^q - x_1, \ldots, x_k^q - x_k\} \subset I$. Then I is zero-dimensional and radical. Let $\mathcal{V}(I) = \{P_1, P_2, \ldots, P_n\}$. We have an isomorphism of $\mathbb{F}_q$ vector spaces (an *evaluation map*):

$$\begin{array}{rcl} \phi : R = \mathbb{F}_q[x_1, \ldots, x_k]/I & \longrightarrow & (\mathbb{F}_q)^n \\ f & \longmapsto & (f(P_1), \ldots, f(P_n)). \end{array} \tag{1}$$

Let $L \subseteq R$ be an $\mathbb{F}_q$ vector subspace of R with dimension r.

Definition 1. *The* **affine–variety code** $C(I, L)$ *is the image* $\phi(L)$ *and the affine–variety code* $C^{\perp}(I, L)$ *is its dual code.*

Our definition is slightly different with respect to that in [1]. Let L be linearly generated by $b_1, \ldots, b_r$ then the matrix

$$H = \begin{pmatrix} b_1(P_1) & b_1(P_2) & \ldots & b_1(P_n) \\ \vdots & \vdots & \ldots & \vdots \\ b_r(P_1) & b_r(P_2) & \ldots & b_r(P_n) \end{pmatrix}$$

is a generator matrix for $C(I,L)$ and a parity–check matrix for $C^{\perp}(I,L)$. Let $\bar{z} \in (\mathbb{F}_q)^n$, $\bar{z} = (\bar{z}_1, \ldots, \bar{z}_n)$. Then

$$\bar{z} \in C(I,L)^{\perp} \iff H\bar{z}^T = 0 \iff \sum_{i=1}^{n} \bar{z}_i b_j(P_i) = 0 \quad j = 1, \ldots, r \tag{2}$$

Proposition 1. *Let $1 \leq w \leq n$.*
Let J_w be the ideal in $\mathbb{F}_q[x_{1,1}, \ldots x_{1,k}, \ldots, x_{w,1}, \ldots x_{w,k}, z_1, \ldots, z_w]$ generated by

$$\sum_{i=1}^{w} z_i b_j(P_i) \quad j = 1, \ldots, r \tag{3}$$

$$g_h(x_{i,1}, \ldots x_{i,k}) \quad i = 1, \ldots, w \text{ and } h = 1, \ldots, s \tag{4}$$

$$z_i^{q-1} - 1 \quad i = 1, \ldots, w \tag{5}$$

$$\prod_{1 \leq l \leq k} ((x_{j,l} - x_{i,l})^{q-1} - 1) \quad 1 \leq j < i \leq w. \tag{6}$$

Then any solution of J_w corresponds to a codeword of $C^{\perp}(I,L)$ with weight w. Moreover,

$$A_w(\mathcal{C}^{\perp}(I,L)) = \frac{|\mathcal{V}(J_w)|}{w!}.$$

Proof. Let σ be a permutation, $\sigma \in S_n$. It induces a permutation $\hat{\sigma}$ acting over $\{x_{1,1}, \ldots, x_{1,k}, \ldots, x_{w,1}, \ldots x_{w,k}, z_1, \ldots, z_w\}$ as $\hat{\sigma}(x_{i,l}) = x_{\hat{\sigma}(i),l}$ and $\hat{\sigma}(z_i) = z_{\hat{\sigma}(i)}$. It is easy to show that J_w is invariant w.r.t. any $\hat{\sigma}$, since each of (3), (4), (5) and (6) is so.
Let $Q = (\overline{x}_{1,1}, \ldots \overline{x}_{1,k}, \ldots, \overline{x}_{w,1}, \ldots \overline{x}_{w,k}, \overline{z}_1, \ldots, \overline{z}_w) \in \mathcal{V}(J_w)$. We can associate a codeword to Q in the following way. For each $i = 1, \ldots, w$, $P_{r_i} = (\overline{x}_{i,1}, \ldots \overline{x}_{i,k})$ is in $\mathcal{V}(I)$, by (4). We can assume $r_1 < r_2 < \ldots < r_w$, via a permutation $\hat{\sigma}$ if necessary. Note that (6) ensures that for each (i,j), with $i \neq j$, we have $P_{r_i} \neq P_{r_j}$, since there is a l such that $x_{i,l} \neq x_{j,l}$. Since $\overline{z}_i^{q-1} = 1$ (5), $\overline{z}_i \in \mathbb{F}_q \setminus \{0\}$.
Let $c \in (\mathbb{F}_q)^n$ be

$$c = (0, \ldots, 0, \underset{\substack{\uparrow \\ P_{r_1}}}{\overline{z}_1}, 0, \ldots, 0, \underset{\substack{\uparrow \\ P_{r_i}}}{\overline{z}_i}, 0, \ldots, 0, \underset{\substack{\uparrow \\ P_{r_w}}}{\overline{z}_w}, 0, \ldots, 0).$$

We have that $c \in \mathcal{C}^{\perp}(I,L)$, since (3) is equal to (2).
Reversing the previous argument, we can associate to any codeword, a solution of J_w. By invariance of J_w, we actually have $w!$ distinct solutions for any codeword. So, to get the number of codewords of weight w, we divide $|\mathcal{V}(J_w)|$ by $w!$.

For more recent results on affine-variety codes see [2,6,4].

2 Hermitian Codes

Hermitian codes are interesting affine–variety codes. They can be defined as follows. Let q be a power of a prime, the *Hermitian curve* $\mathcal{H}$ is the curve defined

over $\mathbb{F}_{q^2}$ by the affine equation

$$x^{q+1} = y + y^q \tag{7}$$

This curve has genus $g = \frac{q(q-1)}{2}$ and has $n = q^3$ rational affine points, denoted by $P_1, \ldots, P_n$. For any $x \in \mathbb{F}_{q^2}$, the equation (7) has exactly q distinct solutions in $\mathbb{F}_{q^2}$. The curve has also one point at infinity P_∞, so it has $q^3 + 1$ rational points over $\mathbb{F}_{q^2}$.

Lemma 1. *Let $\mathcal{L}$ be any vertical line $\{x = t\}$, with $t \in \mathbb{F}_{q^2}$. Then $\mathcal{L}$ intersects $\mathcal{H}$ in q affine points.*

Proof. For any $t \in \mathbb{F}_{q^2}$, the equation $y^q + y = t^{q+1}$ has exactly q distinct solutions, since $t^{q+1} \in \mathbb{F}_q$ and the trace is linear.

Lemma 2. *In the affine plane $(\mathbb{F}_{q^2})^2$, the total number of non-vertical line is q^4. Of these, $(q^4 - q^3)$ intersect the Hermitian curve in $(q+1)$ points and q^3 are tangent to $\mathcal{H}$, i.e. they intersect $\mathcal{H}$ in one point.*

Proof. Let $\mathcal{L}$ any non-vertical line, $\mathcal{L} = \{y = ax + b\}$. We have q^2 choice for both a and b, so the total number is q^4. Then

$$\mathcal{H} \cap \mathcal{L} = \{(x, ax + b) \mid a^q x^q + b^q + ax + b = x^{q+1}\}.$$

Let $c = a^{q+1} + b^q + b$. We have two distinct cases:

- $c = 0$. Then $a^q x^q + b^q + ax + b = x^{q+1}$ becomes $a^q x^q - a^{q+1} + ax = x^{q+1}$, which gives $x = a^q$, that is, $\mathcal{L}$ is tangent.
- $c \neq 0$. Then $a^q x^q + b^q + ax + b = x^{q+1}$ becomes $x^{q+1} - a^q x^q + a^{q+1} - ax = c$, which gives $(x - a^q)^{q+1} = c$. Since $c = (\alpha^{q+1})^r$ for $1 \leq r \leq q - 1$, we have $x = a^q + \alpha^{r+i(q-1)}$ for any $0 \leq i \leq q$.

The number of pairs (a, b) satisfying $c = 0$ is q^3 and so the others are $(q^4 - q^3)$.

Let $I = \langle y^q + y - x^{q+1}, x^{q^2} - x, y^{q^2} - y \rangle \subset \mathbb{F}_{q^2}[x, y]$ and let $R = \mathbb{F}_{q^2}[x, y]/I$. We take $L \subseteq R$ generated by

$$\mathcal{B}_{m,q} = \{x^r y^s + I \mid qr + (q+1)s \leq m,\ 0 \leq s \leq q - 1,\ 0 \leq r \leq q^2 - 1\},$$

where m is an integer $0 \leq m \leq q^3 + q^2 - q - 2$. For simplicity, we also write $x^r y^s$ for $x^r y^s + I$. We consider the evaluation map (1) $\phi : R \to (\mathbb{F}_{q^2})^n$. We have the following affine–variety codes $C(I, L) = \mathrm{Span}_{\mathbb{F}_{q^2}} \langle \phi(\mathcal{B}_{m,q}) \rangle$ and we denote by $C(m, q) = (C(I, L))^\perp$ its dual. Then the affine–variety code $C(m, q)$ is called the *Hermitian code* with parity-check matrix H

$$H = \begin{pmatrix} f_1(P_1) & \ldots & f_1(P_n) \\ \vdots & \ddots & \vdots \\ f_i(P_1) & \ldots & f_i(P_n) \end{pmatrix} \text{ where } f_j \in \mathcal{B}_{m,q} \tag{8}$$

The Hermitian codes can be divided in four phases ([3]), any having specific explicit formulae linking their dimension and their distance, as in Table 1.
In the remainder of this paper we focus on the first phase. This case can be characterised by the condition $d \leq q$.

Table 1. The four phases of Hermitian codes

Phase	m	Distance d	Dimension k
1	$0 \le m \le q^2-2$ $m = aq+b$ $0 \le b \le a \le q-1$ $b \le q-2$	$a+1\ a > b$ $a+2\ a = b$ $\iff d \le q$	$q^3 - \frac{a(a+1)}{2} - (b+1)$
2	$q^2-1 \le m \le 2q^2-2q-2$ $m = 2q^2-q-aq-b-1$ $1 \le a \le q-1$ $0 \le b \le q-1$	$(q-a)q-b \quad a < b$ $(q-a)q \quad\ a \ge b$	$q^3 - m + \frac{q(q-1)}{2} - 1$
3	$2q^2-2q-1 \le m \le q^3-1$	$m-q^2+q+1$	$q^3 - m + \frac{q(q-1)}{2} - 1$
4	$q^3 \le m < q^3+q^2-q-1$ $m = q^3+aq+b$ $0 \le a \le q-1,$ $0 \le b \le q-2$	$q^3+aq+b-2g \quad a < b$ $q^3+aq+a+1-2g\ b \le a$	$k \ge g-aq-b$

2.1 Corner Codes and Edge Codes

The first-phase Hermitian codes can be either *edge codes* or *corner codes*.

Definition 2. *Let* $2 \le d \le q$ *and let* $1 \le j \le d-1$.
Let $L_0^d = \{1, x, \ldots, x^{d-2}\}, L_1^d = \{y, xy, \ldots, x^{d-3}y\}, \ldots, L_{d-2}^d = \{y^{d-2}\}$.
Let $l_1^d = x^{d-1}, \ldots, l_j^d = x^{d-j}y^{j-1}$.

- *If* $\mathcal{B}_{m,q} = L_0^d \sqcup \cdots \sqcup L_{d-2}^d$, *then we say that* $C(m,q)$ *is a* ***corner code*** *and we denote it by* H_d^0.
- *If* $\mathcal{B}_{m,q} = L_0^d \sqcup \cdots \sqcup L_{d-2}^d \sqcup \{l_1^d, \ldots, l_j^d\}$, *then we say that* $C(m,q)$ *is an* ***edge code*** *and we denote it by* H_d^j.

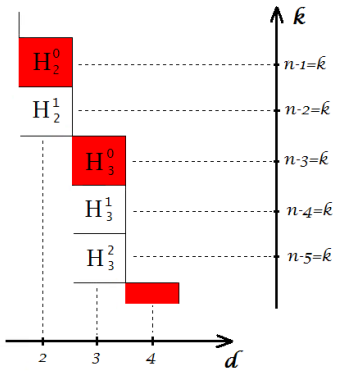
From classical results in Table 1 we have

Theorem 1. *Let* $2 \le d \le q$, $1 \le j \le d-1$. *Then*

$$d(H_d^0) = d(H_d^j) = d,\ \dim_{\mathbb{F}_{q^2}}(H_d^0) = n - \frac{d(d-1)}{2},\ \dim_{\mathbb{F}_{q^2}}(H_d^j) = n - \frac{d(d-1)}{2} - j$$

In other words, all $\phi(x^r y^s)$ are linearly independent (i.e. H has maximal rank) and for any distance d there are exactly d Hermitian codes (one corner code and $d-1$ edge codes). We can represent the above codes as in the following picture, where we consider the five smallest non-trivial codes (for any $q \ge 3$).

H_2^0 is a $[n, n-1, 2]$ code.
$\mathcal{B}_{m,q} = L_0^2 = \{1\}$, so the parity-check matrix of H_2^0 is $(1, \ldots, 1)$.
H_2^1 is a $[n, n-2, 2]$ code.
$\mathcal{B}_{m,q} = L_0^2 \sqcup l_1^2 = \{1, x\}$
H_3^0 is a $[n, n-3, 3]$ code.
$\mathcal{B}_{m,q} = L_0^3 \sqcup L_1^3 = \{1, x, y\}$
H_3^1 is a $[n, n-4, 3]$ 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 a $[n, n-5, 3]$ code.
$\mathcal{B}_{m,q} = L_0^3 \sqcup L_1^3 \sqcup \{l_1^3, l_2^3\} = \{1, x, y, x^2, xy\}$



3 Our results on the number of words

Ideal J_w of Proposition 1 for $C(m, q)$ is

$$J_w = \Big\langle \Big\{ \sum_{i=1}^{w} z_i x_i^r y_i^s \Big\}_{x^r y^s \in \mathcal{B}_{m,q}}, \Big\{ x_i^{q+1} - y_i^q - y_i \Big\}_{i=1,\ldots,w}, \Big\{ z_i^{q^2-1} - 1 \Big\}_{i=1,\ldots,w}, \Big\{ x_i^{q^2} - x_i \Big\}_{i=1,\ldots,w}, \Big\{ y_i^{q^2} - y_i \Big\}_{i=1,\ldots,w}, \Big\{ \prod_{1 \le i < j \le w} ((x_i - x_j)^{q^2-1} - 1)((y_i - y_j)^{q^2-1} - 1) \Big\} \Big\rangle. \quad (9)$$

Let $w \ge v \ge 1$. Let $Q = (\overline{x}_1, \ldots, \overline{x}_w, \overline{y}_1, \ldots, \overline{y}_w, \overline{z}_1, \ldots, \overline{z}_w) \in \mathcal{V}(J_w)$. We say that Q is in **v-block position** if we can partition $\{1, \ldots, n\}$ in v blocks $I_1, \ldots, I_v$ such that

$$\overline{x}_i = \overline{x}_j \iff \exists\, 1 \le h \le v \text{ such that } i, j \in I_h.$$

W.l.o.g. we can assume $|I_1| \le \cdots \le |I_v|$ and $I_1 = \{1, \ldots, u\}$. It is simple to prove the following numerical lemma.

Lemma 3. *We always have $u + v \le w + 1$. If $u \ge 2$ and $v \ge 2$, then $v \le \lfloor \frac{w}{2} \rfloor$ and $u + v \le \lfloor \frac{w}{2} \rfloor + 2$.*

We need the following technical lemma [7].

Lemma 4. *Let us consider the edge code H_d^j with $1 \le j \le d-1$ and $3 \le d \le w \le 2d-3$. Let $Q = (\overline{x}_1, \ldots, \overline{x}_d, \overline{y}_1, \ldots, \overline{y}_d, \overline{z}_1, \ldots, \overline{z}_d)$ be a solution of J_w in v-block position, with $v \le w$, then exactly one of the following cases holds*

(a) $u = 1 \quad v > d \quad w \ge d+1$
(b) $v = 1$, *that is,* $\bar{x}_1 = \cdots = \bar{x}_w$

If $d = 2$ and $w = 2$, then (a) holds for H_2^1.

Proof. We denote for all $1 \le h \le v$

$$X_h = \bar{x}_i \text{ if } i \in I_h, \quad Z_h = \sum_{i \in I_h} \bar{z}_i, \quad Y_{h,\delta} = \sum_{i \in I_h} \bar{y}_i^{\delta} \bar{z}_i \text{ with } 1 \le \delta \le u-1$$

(a) $u = 1$. We have to prove, by contradiction, that $v > d$.
Let $v \leq d$. Since $Q \in \mathcal{V}(J_w)$, then $L_0^w(Q) = l_1^w(Q) = 0$, that is

$$0 = \sum_{i=1}^{w} \bar{x}_i^r \bar{z}_i = \sum_{i \in I_h} X_h^r \bar{z}_i = \sum_{h=1}^{v} X_h^r Z_h \quad 0 \leq r \leq d-1. \tag{10}$$

We can consider only the first v equations of (10), because $v \leq d$, so

$$\sum_{h=1}^{v} X_h^r Z_h = 0 \quad 0 \leq r \leq v-1 \iff \begin{pmatrix} 1 & \dots & 1 \\ X_1 & \dots & X_v \\ \vdots & \dots & \vdots \\ X_1^{v-1} & \dots & X_v^{v-1} \end{pmatrix} \begin{pmatrix} Z_1 \\ \vdots \\ Z_v \end{pmatrix} = 0 \tag{11}$$

The above matrix is a Vandermonde matrix, so it has maximal rank v. Therefore, the solution of (11) is $(Z_1, \dots, Z_v) = (0, \dots, 0)$. Since $u = 1$, then $Z_1 = \bar{z}_1 = 0$, which contradicts $\bar{z}_i \in \mathbb{F}_{q^2} \setminus \{0\}$. So if $v > d$ then $w \geq d + 1$.

(b) $u \geq 2$. We suppose by contradiction that $v \geq 2$.
We consider Proposition 1. A subset of equations of condition (3) is the following system, where $0 \leq r \leq v$

$$\begin{cases} \sum_{i=1}^{w} \bar{x}_i^r \bar{z}_i = 0 \\ \sum_{i=1}^{w} \bar{x}_i^r \bar{y}_i \bar{z}_i = 0 \\ \quad \vdots \\ \sum_{i=1}^{w} \bar{x}_i^r \bar{y}_i^{u-1} \bar{z}_i = 0 \end{cases} \iff \begin{cases} \sum_{h=1}^{v} X_h^r Z_h = 0 \\ \sum_{h=1}^{v} X_h^r Y_{h,1} = 0 \\ \quad \vdots \\ \sum_{h=1}^{v} X_h^r Y_{h,u-1} = 0 \end{cases} \tag{12}$$

In fact system (12) is a subset of (3) if and only if $\deg(\bar{x}_i^v \bar{y}_i^{u-1}) \leq d-1$ for any $i = 1, \dots, w$. That is, $v + (u-1) \leq d-1 \iff v + u \leq d$. To verify it, since $v \geq 2$, it is sufficient to apply Lemma 3 and we obtain $u + v \leq \lfloor \frac{w}{2} \rfloor + 2 \leq \lfloor \frac{2d-3}{2} \rfloor + 2 = d$.
By system (12) we obtain u Vandermonde matrices (all having rank v). Therefore the solutions of these matrices are zero-solutions. So, in the particular case $h = 1$, we have $Z_1 = Y_{1,1} = \dots = Y_{1,u-1} = 0$, that is

$$\begin{cases} \sum_{i=0}^{u} \bar{z}_i = 0 \\ \sum_{i=0}^{u} \bar{y}_i \bar{z}_i = 0 \\ \quad \vdots \\ \sum_{i=0}^{u} \bar{y}_i^{u-1} \bar{z}_i = 0 \end{cases} \iff \begin{pmatrix} 1 & \dots & 1 \\ \bar{y}_1 & \dots & \bar{y}_u \\ \vdots & \dots & \vdots \\ \bar{y}_1^{u-1} & \dots & \bar{y}_u^{u-1} \end{pmatrix} \begin{pmatrix} \bar{z}_1 \\ \vdots \\ \bar{z}_u \end{pmatrix} = 0$$

Since the $\bar{y}_i$'s are all distinct (because the $\bar{x}_i$'s are all equal), we obtain a Vandermonde matrix, and so $\bar{z}_1 = \dots = \bar{z}_u = 0$, but it is impossible because $\bar{z}_i \in \mathbb{F}_{q^2} \setminus \{0\}$. Therefore $v = 1$.

The case H_2^1 is trivial.

Corollary 1. *Let us consider the edge code H_d^j with $1 \leq j \leq d-1$.*
If $Q = (\overline{x}_1, \ldots, \overline{x}_d, \overline{y}_1, \ldots, \overline{y}_d, \overline{z}_1, \ldots, \overline{z}_d) \in \mathcal{V}(J_d)$, then $\bar{x}_1 = \cdots = \bar{x}_d$. In other words, the points that correspond to a minimum-weight word lie in the intersection of the Hermitian curve $\mathcal{H}$ and one vertical line.
Whereas if $d \geq 4$ and $Q = (\overline{x}_1, \ldots, \overline{x}_{d+1}, \overline{y}_1, \ldots, \overline{y}_{d+1}, \overline{z}_1, \ldots, \overline{z}_{d+1}) \in \mathcal{V}(J_{d+1})$, then one of the following cases holds

(a) $\bar{x}_i \neq \bar{x}_j$ con $i \neq j$ per $1 \leq i, j \leq d+1$
(b) $\bar{x}_1 = \cdots = \bar{x}_{d+1}$.

Proof. We are in the hypotheses of Lemma 4. So if $w = d$ then $u \neq 1$. So $v = 1$. Whereas, if $w = d+1$ then there are two possibilities. In case (a) of Lemma 4, all the $\bar{x}_i$'s are different, since $v = d+1$, or, case (b), $\bar{x}_1 = \cdots = \bar{x}_{d+1}$.

Now we can prove the following theorem.

Theorem 2. *The number of minimum weight words of an edge code H_d^j is*

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

Proof. By Proposition 1 we know that J_d represents all words of minimum weight. The first set of ideal basis (9) has exactly $\frac{d(d-1)}{2} + j$ equations, where $1 \leq j \leq d-1$. So, if $j = 1$, this set implies the following system:

$$\begin{cases} \bar{z}_1 + \cdots + \bar{z}_d = 0 \\ \bar{x}_1\bar{z}_1 + \cdots + \bar{x}_d\bar{z}_d = 0 \\ \bar{y}_1\bar{z}_1 + \cdots + \bar{y}_d\bar{z}_d = 0 \\ \bar{x}_1^2\bar{z}_1 + \cdots + \bar{x}_d^2\bar{z}_d = 0 \\ \quad \vdots \\ \bar{y}_1^{d-2}\bar{z}_1 + \cdots + \bar{y}_d^{d-2}\bar{z}_d = 0 \\ \bar{x}_1^{d-1}\bar{z}_1 + \cdots + \bar{x}_d^{d-1}\bar{z}_d = 0 \end{cases} \tag{13}$$

Whereas, if $j > 1$ then we have to add the first $j-1$ of following equations:

$$\begin{cases} \bar{x}_1^{d-2}\bar{y}_1\bar{z}_1 + \cdots + \bar{x}_d^{d-2}\bar{y}_d\bar{z}_d = 0 \\ \quad \vdots \\ \bar{x}_1\bar{y}_1^{d-2}\bar{z}_1 + \cdots + \bar{x}_d\bar{y}_d^{d-2}\bar{z}_d = 0 \end{cases}$$

But $\bar{x}_1 = \ldots = \bar{x}_d$, since we are in the hypotheses of Corollary 1. So the system becomes

$$\begin{cases} \bar{z}_1 + \cdots + \bar{z}_d = 0 \\ \bar{y}_1\bar{z}_1 + \cdots + \bar{y}_d\bar{z}_d = 0 \\ \quad \vdots \\ \bar{y}_1^{d-2}\bar{z}_1 + \cdots + \bar{y}_d^{d-2}\bar{z}_d = 0 \end{cases} \tag{14}$$

We have q^2 choice for the $\bar{x}_i$'s and, by Lemma 1, we have $\binom{q}{d} d!$ different $\bar{y}_i$'s, since for any choice of the $\bar{x}_i$'s there are exactly q possible value for the $\bar{y}_i$'s, but

we need just d of them and any permutation of these will be again a solution. Now we have to calculate the solutions for the $\bar{z}_i$'s.
We write the system (14) as a matrix, which is a Vandermonde matrix with rank $d-1$. This means that the solution space has linear dimension 1 because $1 = d - (d-1) =$ number of variables $-$ rank of matrix. So the solutions are $(a_1\alpha, a_2\alpha, \ldots, a_{d-1}\alpha)$ with $\alpha \in \mathbb{F}_{q^2}^*$, where a_j are fixed since they depend on $\bar{y}_i$. So the number of the z's is $|\mathbb{F}_{q^2}^*| = q^2 - 1$, then $A_d = \frac{1}{d!}\left(q^2(q^2-1)\binom{q}{d}d!\right)$.

We consider a corner code. We have the following geometric characterisation.

Proposition 2. *Let us consider the corner code H_d^0, then the points $(\bar{x}_1, \bar{y}_1), \ldots, (\bar{x}_d, \bar{y}_d)$ corresponding to minimum-weight words lie on the same line.*

Proof. The minimum-weight words of a corner code have to verify the first condition set of J_w, which has $\frac{d(d-1)}{2}$ equations. That is

$$\begin{cases} \bar{z}_1 + \cdots + \bar{z}_d = 0 \\ \bar{x}_1\bar{z}_1 + \cdots + \bar{x}_d\bar{z}_d = 0 \\ \bar{y}_1\bar{z}_1 + \cdots + \bar{y}_d\bar{z}_d = 0 \\ \bar{x}_1^2\bar{z}_1 + \cdots + \bar{x}_d^2\bar{z}_d = 0 \\ \quad\vdots \\ \bar{y}_1^{d-2}\bar{z}_1 + \cdots + \bar{y}_d^{d-2}\bar{z}_d = 0 \end{cases} \tag{15}$$

This system is the same as (13), but with a missing equation. This means that (15) have all solutions of system (13) plus other solutions.
If we consider a subset of (15):

$$\begin{cases} \bar{z}_1 + \cdots + \bar{z}_d = 0 \\ \bar{x}_1\bar{z}_1 + \cdots + \bar{x}_d\bar{z}_d = 0 \\ \bar{x}_1^2\bar{z}_1 + \cdots + \bar{x}_d^2\bar{z}_d = 0 \\ \quad\vdots \\ \bar{x}_1^{d-2}\bar{z}_1 + \cdots + \bar{x}_d^{d-2}\bar{z}_d = 0 \end{cases} \tag{16}$$

we note that the $\bar{z}_i$'s are all non-zero if all $\bar{x}_i$'s are distinct (or all are equal). Therefore, we have only two possibilities for the $\bar{x}_i$'s: either are all different or they coincide. The same consideration is true for the $\bar{y}_i$'s, in fact when we consider (15) and we exchange x with y, we obtain again (15).
So we have an alternative:

- The $\bar{x}_i$'s are all equal or the $\bar{y}_i$'s are all equal, so our proposition is true.
- The $\bar{x}_i$'s and the $\bar{y}_i$'s are all distinct. We prove that they line in the intersection of a non-horizontal line.
  Let $y = \beta x + \lambda$ be a non-vertical line passing for two points in a minimum weight configuration. We can do an affine transformation of this type:

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

such that some of the y''s are equal and not all y's are coincident. Substituting the above transformation in (15) and applying some operations between the equations, we obtain a system that is equivalent to (15). But this new system have all y''s equal (or all distinct), so the y''s have to be all equal. Hence we can conclude that the points lie on the same line.

We finally prove the following theorem:

Theorem 3. *The number of words having weight d of a corner code H_d^0 is*

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

Proof. Again, the points corresponding to minimum-weight words of a corner code have to verify (15). By above proposition, we know that these points lie in the intersections of any line and the Hermitian curve $\mathcal{H}$.
Let $Q = (\overline{x}_1, \ldots, \overline{x}_d, \overline{y}_1, \ldots, \overline{y}_d, \overline{z}_1, \ldots, \overline{z}_d) \in \mathcal{V}(J_d)$ such that $\overline{x}_1 = \ldots = \overline{x}_d$, that is, the points $(\bar{x}_i, \bar{y}_i)$ lie on a vertical line. We know that the number of such Q's is $q^2(q^2-1)\binom{q}{d} d\,!$. Now we have to calculate the number of solutions $Q \in \mathcal{V}(J_d)$ such that $(\bar{x}_i, \bar{y}_i)$ lie on a non-vertical line.
By Lemma 2 we know that the number of the $\bar{y}_i$'s and $\bar{x}_i$'s is $(q^4-q^3)\binom{q+1}{d} d\,!$, since for any choice of the $\bar{y}_i$'s there are exactly $q+1$ possible values for the $\bar{x}_i$'s, but we need just d of this (and the system is invariant). As regards the number of the $\bar{z}_i$'s, we have to calculate the number of solutions of system (15).
We apply an affine transformation to the system (15) to obtain a horizontal line, that is, to have all the $\bar{y}_i$'s different and all the $\bar{x}_i$'s are equal, so we obtain a system equivalent to system (14). Therefore we have a Vandermonde matrix, hence the number of the $\bar{z}_i$'s is q^2-1. So

$$\begin{aligned} A_d &= \tfrac{1}{d!}\left(q^2(q^2-1)\binom{q}{d} d\,! + (q^4-q^3)(q^2-1)\binom{q+1}{d} d\,!\right) \\ &= q^2(q^2-1)\binom{q}{d-1}\tfrac{q^3-d+1}{d}. \end{aligned}$$

3.1 Words having weight $d+1$

In this section we state more theorems for edge and corner codes taken from [5]. We study the case when the x_i's coincide or when the y_i's coincide.

Theorem 4. *The number of words of weight $d+1$ with $y_1 = \ldots = y_{d+1}$ of a corner code H_d^0 is:*

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

Whereas of an edge code H_d^j with $1 \le j \le d-1$ is:

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

Theorem 5. *The number of words of weight $d+1$ with $x_1 = \ldots = x_{d+1}$ 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 proofs are similar to those of the statements as in Section 3 and so are omitted. In other cases, we have to consider intersection of the curve with higher degree curves and the formulae get more complicated. We list without proof a few of these special cases:

Theorem 6. *Let us consider the corner code H_3^0. Let us consider 4-weight codewords with $x_i \neq x_j$ for any $i, j = 1, \ldots, 4$. Then*

$\mathbf{y_1} = \mathbf{y_2} = \mathbf{y_3} \neq \mathbf{y_4}$	$A_4 = 0$
$\mathbf{y_1} = \mathbf{y_2} \neq \mathbf{y_3} = \mathbf{y_4}$	$A_4 = \frac{1}{8}q^2(q^2-1)^2(q-2)(q^3+2q^2-2q+1)$
$\mathbf{y_1} = \mathbf{y_2} \neq \mathbf{y_3}, \mathbf{y_4}$	$A_4 > \frac{1}{4}q^2(q^2-1)^2(2q^6-7q^5-6q^4+19q^3-9q^2-4q+4)$
and $\mathbf{y_3} \neq \mathbf{y_4}$	$A_4 < \frac{1}{4}q^2(q^2-1)^2(2q^6-3q^5-11q^4+9q^3+25q^2-14q+4)$

Theorem 7. *Let us consider the edge codes H_3^1 and H_3^2. Let us consider 4-weight codewords with $x_i \neq x_j$ for any $i, j = 1, \ldots, 4$. Then there are no such words if $y_1 = y_2 = y_3 \neq y_4$ or $y_1 = y_2 \neq y_3 = y_4$.*
In particular, if $y_1 = y_2 \neq y_3, y_4$ and $y_3 \neq y_4$, H_3^2 has no such words and H_3^1 has at most $\frac{1}{4}q^2(q^2-1)^2(2q^5-3q^4-10q^3+10q^2+15q-4)$ such words.

Remark 1. We are identifying general conditions for algebraic-geometry codes satisfying Proposition 2, jointly with C. Fontanari.

Acknowledgements

The first two authors would like to thank their supervisor: the third author. The authors would like to thank: C. Fontanari, T. Mora and C. Traverso.

References

1. Fitzgerald, J. and Lax, R. F. *Decoding affine variety codes using Gröbner bases.* Des. Codes Cryptogr., 1998.
2. Geil, O. *Evaluation codes from an affine-variety codes perspective, pagg. 153-180.* in *Advances in Algebraic Geometry codes*, eds (E. Martinez-Moro, C. Munuera, D. Ruano), World Scientific, 2008.
3. Høholdt, T. and van Lint, J. H. and Pellikaan, R. *Algebraic geometry of codes, pagg. 871–961.* North-Holland, 1998.
4. Lax, R. F. *Generic interpolation polynomial for list decoding*, to appear, 2011.
5. Marcolla, C. *Parole di peso piccolo dei codici hermitiani.* Tesi di laurea, 2009.
6. Marcolla, C. and Orsini, E. and Sala, M. *Improved decoding of affine–variety codes*, arXiv preprint `http://arxiv.org/abs/1102.4186`.
7. Pellegrini, M. *On the weight distribution of some Goppa AG codes.* Ph.D. thesis, University of Pisa, Work in progress.