On the small weights codewords of some Hermitian codes

Chiara Marcolla (chiara.marcolla@unitn.it)
Department of Mathematics, University of Trento, Italy

Marco Pellegrini (pellegrin@math.unifi.it)
Department of Mathematics, University of Firenze, Italy

Massimiliano Sala (maxsalacodes@gmail.com)
Department of Mathematics, University of Trento, Italy

Abstract

For any affine-variety code we show how to construct an ideal whose solutions correspond to codewords with any assigned weight. We are able to obtain geometric characterizations for small-weight codewords for some families of Hermitian codes over any $\mathbb{F}_{q^2}$. From these geometric characterizations, we obtain explicit formulas. In particular, we determine the number of minimum-weight codewords for all Hermitian codes with $d \leq q$ and all second-weight codewords for distance-3, 4 codes.

Keywords: Affine-variety code, hamming weight, Hermitian code, Hermitian curve, linear code, minimum-weight words.

1 Introduction

Let $q$ be a power of a prime, then the Hermitian curve $H$ is the plane curve defined over $\mathbb{F}_{q^2}$ by the affine equation $x^{q+1} = y^q + y$, where $x, y \in \mathbb{F}_{q^2}$.

This curve has genus $g = \frac{q(q-1)}{2}$ and has $q^3 \mathbb{F}_{q^2}$-rational affine points, plus one point at infinity, so it has $q^3 + 1$ rational points over $\mathbb{F}_{q^2}$ and therefore it is a maximal curve [RS94]. This is the best known example of maximal curve and there is a vast literature on its properties, see [HKT08] for a recent survey. Moreover, the Goppa code [Gop88] constructed on this curve is by far the most studied, due to the simple basis of its Riemann-Roch space [Sti93], which can be written explicitly. The Goppa construction has been generalized in [FL98] to the so-called affine-variety codes.

In this paper we provide an algebraic and geometric description for codewords of a given weight belonging to any fixed affine-variety codes. The specialization of our results to the Hermitian case permits us to give explicit
formulas for the number of some small-weight codewords. We expand on our 2006 previous result [SP06], where we proved the intimate connection between curve intersections and minimum-weight codewords.

The paper is organized as follows:

- In Section 2 we provide our notation, our first preliminary results on the algebraic characterization of fixed-weight codewords of any-affine variety codes and some easy results on the intersection between the Hermitian curve and any line.

- In the beginning of Section 3 we provide a division of Hermitian codes in four phases, which is a slight modification of the division in [HvLP98], and we give our algebraic characterization of fixed-weight codewords of some Hermitian codes. We study in deep the first phase (that is, \( d \leq q \)) in Subsection 3.2 and we use these results to completely classify geometrically the minimum-weight codewords for all first-phase codes in Subsection 3.3. In Subsection 3.4 we can count some special configurations of second weight codewords for any first-phase code and finally in Subsection 3.5 we can count the exact number of second-weight codewords for the special case when \( d = 3, 4 \). A result in this section rely on our results [MPS12] on intersection properties of \( \mathcal{H} \) (with some special conics), presented at Effective Method in Algebraic Geometry, MEGA 2013.

- In Section 4 we draw some conclusions and propose some open problems.

2 Preliminary results

2.1 Known facts on Hermitian curve and Affine-variety code

From now on we consider \( \mathbb{F}_{q^2} \) the finite field with \( q^2 \) elements, and \( \mathbb{F}_q \) the finite field with \( q \) elements, where \( q \) is a power of a prime. Let \( \alpha \) be a fixed primitive element of \( \mathbb{F}_{q^2} \), and we consider \( \beta = \alpha^{q+1} \) as a primitive element of \( \mathbb{F}_q \). From now on \( q, q^2, \alpha \) and \( \beta \) are understood as above.

The **Hermitian curve** \( \mathcal{H} = \mathcal{H}_q \) is defined over \( \mathbb{F}_{q^2} \) by the affine equation

\[
x^{q+1} = y^q + y \quad \text{where } x, y \in \mathbb{F}_{q^2}.
\]  

(1)

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 (1) has exactly \( q \) distinct solutions in \( \mathbb{F}_{q^2} \). The curve contains also one point at infinity \( P_{\infty} \), so it has \( q^3 + 1 \) rational points over \( \mathbb{F}_{q^2} \) [RS94].

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 \( \mathcal{V}(I) \subset (\mathbb{F}_q)^k \) its variety, that is, the set of its common roots. For any \( Z \subset (\mathbb{F}_q)^k \) we denote by \( \mathcal{I}(Z) \subset \mathbb{F}_q[X] \) the vanishing
ideal of $Z$, that is, $I(Z) = \{ f \in \mathbb{F}_q[x] \mid f(Z) = 0 \}$.

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 $\{x_i^q - x_i, \ldots, x_k^q - x_k\} \subset I$. Then $I$ is zero-dimensional and radical [Sei74]. Let $\mathcal{V}(I) = \{P_1, \ldots, P_n\}$. We have an isomorphism of $\mathbb{F}_q$ vector spaces (an evaluation map):

$$
\phi : R = \mathbb{F}_q[x_1, \ldots, x_k]/I \longrightarrow (\mathbb{F}_q)^n
$$

$$
f \longmapsto (f(P_1), \ldots, f(P_n)). \tag{2}
$$

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

**Definition 2.1.** 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 from [FL98] and follows instead that in [MOS12]. Let $L$ be linearly generated by $b_1, \ldots, b_r$ then the matrix

$$
H = \begin{pmatrix}
\begin{array}{cccc}
b_1(P_1) & b_1(P_2) & \cdots & b_1(P_n) \\
\vdots & \vdots & \ddots & \vdots \\
b_r(P_1) & b_r(P_2) & \cdots & b_r(P_n)
\end{array}
\end{pmatrix}
$$

is a generator matrix for $C(I, L)$ and a parity–check matrix for $C^\perp(I, L)$.

For more recent results on affine-variety codes see [Gei08, MOS12, Lax12].

### 2.2 First results on words of given weight

Let $0 \leq w \leq n$, $C$ be a linear code and $c \in C$. We recall that the weight of $c$, denoted by $w(c)$, is the number of components of $c$ that are different to zero and

$$
A_w(C) = |\{c \in C \mid w(c) = w\}|.
$$

Let $\bar{z} \in (\mathbb{F}_q)^n$, $\bar{z} = (\bar{z}_1, \ldots, \bar{z}_n)$. Then

$$
\bar{z} \in C(I, L)^\perp \iff H\bar{z}^T = 0 \iff \sum_{i=1}^n \bar{z}_i b_j(P_i) = 0, \quad j = 1, \ldots, r. \tag{3}
$$

**Proposition 2.2 ([Pel06]).** Let $1 \leq w \leq n$. 

CGC
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

\[
\sum_{i=1}^{w} z_i b_j(x_{i,1}, \ldots, x_{i,k}) \quad \text{for} \quad j = 1, \ldots, r \tag{4}
\]

\[
g_h(x_{i,1}, \ldots, x_{i,k}) \quad \text{for} \quad i = 1, \ldots, s \quad \text{and} \quad h = 1, \ldots, s \tag{5}
\]

\[
z_i^{q-1} - 1, \quad i = 1, \ldots, w \tag{6}
\]

\[
\prod_{1 \leq l \leq k} ((x_{j,l} - x_{i,l})^{q-1} - 1), \quad 1 \leq j < i \leq w. \tag{7}
\]

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

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

**Proof.** Let \( \sigma \) be a permutation, \( \sigma \in S_w \). It induces a permutation \( \hat{\sigma} \) acting on \( \{x_{1,1}, \ldots, x_{1,k}, \ldots, x_{w,1}, \ldots x_{w,k}, z_1, \ldots, z_w\} \) as \( \hat{\sigma}(x_{i,l}) = x_{\sigma(i),l} \) and \( \hat{\sigma}(z_i) = z_{\sigma(i)} \). It is easy to show that \( J_w \) is invariant w.r.t. any \( \hat{\sigma} \), since each of (4), (5), (6) and (7) is so.

Let \( Q = (\mathbf{z}_{1,k}, \ldots, \mathbf{z}_{w,k}, \mathbf{z}_1, \ldots, \mathbf{z}_w) \in \mathcal{V}(J_w) \). We can associate a codeword to \( Q \) in the following way. For each \( i = 1, \ldots, w \), \( P_i = (\mathbf{x}_{i,1}, \ldots, \mathbf{x}_{i,k}) \) is in \( \mathcal{V}(I) \), by (5). We can assume \( r_1 < r_2 < \cdots < r_w \), via a permutation \( \hat{\sigma} \) if necessary. Note that (7) 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 \( \mathbf{x}_{i,l}^{q-1} = 1 \) (6), \( \mathbf{z}_i \in \mathbb{F}_q \setminus \{0\} \).

Let \( c \in (\mathbb{F}_q)^n \) be

\[
c = (0, \ldots, 0, \mathbf{z}_1, 0, \ldots, 0, \mathbf{z}_1, 0, \ldots, 0, \mathbf{z}_w, 0, \ldots, 0).
\]

We have that \( c \in C^\perp(I, L) \), since (4) is equivalent to (3).

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 \( w! \). \( \square \)

Note that this approach is a generalization of the approach in [Sal07] to determine the number of words having given weight for a cyclic code.

### 2.3 Intersection between the Hermitian curve \( \mathcal{H} \) and a line

We consider the norm and the trace, the two functions defined as follows.

**Definition 2.3.** The **norm** \( N_{\mathbb{F}_q}^{F_{q^m}} \) and the **trace** \( Tr_{\mathbb{F}_q}^{F_{q^m}} \) are two functions from \( \mathbb{F}_{q^m} \) to \( \mathbb{F}_q \) such that

\[
N_{\mathbb{F}_q}^{F_{q^m}}(x) = x^{1+q+\cdots+q^{m-1}} \quad \text{and} \quad Tr_{\mathbb{F}_q}^{F_{q^m}}(x) = x + x^q + \cdots + x^{q^{m-1}}.
\]
We denote with $N$ and $\text{Tr}$, respectively, the norm and the trace from $F_{q^2}$ to $F_q$. It is clear that $\mathcal{H} = \{N(x) = \text{Tr}(y) \mid x, y \in F_{q^2}\}$.

We can define a similar curve $\mathcal{H}' = \{N(x) = -\text{Tr}(y) \mid x, y \in F_{q^2}\}$ and, using the next lemma, it is easy to see that also $\mathcal{H}'$ contains $q^3$ affine rational points. A well-known fact is the following [LN86].

**Lemma 2.4.** For any $t \in F_q$, the equation $\text{Tr}(y) = y^q + y = t$ has exactly $q$ distinct solutions in $F_{q^2}$. The equation $N(x) = x^{q+1} = t$ has exactly $q + 1$ distinct solutions, if $t \neq 0$, otherwise it has just one solution.

**Proof.** The trace is a linear surjective function between two $F_q$-vector spaces of dimension, respectively, 2 and 1. Thus, $\dim(\ker(\text{Tr})) = 1$, and this means that for any $t \in F_q$ the set of solutions of the equation $\text{Tr}(y) = y^q + y = t$ is non-empty and then it has the same cardinality of $F_q$, that is, $q$.

The equation $x^{q+1} = 0$ has obviously only the solution $x = 0$. If $t \neq 0$, since $t \in F_q$, we can write $t = \beta^q$, so that $x = \alpha^{q+j(q-1)}$ are all solutions. We can assign $j = 0, \ldots, q$, and so we have $q + 1$ distinct solutions. \qed

**Lemma 2.5.** Let $\mathcal{L}$ be any horizontal line $\{x = t\}$, with $t \in F_{q^2}$. Then $\mathcal{L}$ intersects $\mathcal{H}$ in $q$ affine points.

**Proof.** For any $t \in F_{q^2}$, $t^{q^2+1} \in F_q$, and so the equation $y^q + y = t^{q^2+1}$ has exactly $q$ distinct solutions by applying Lemma 2.4. \qed

**Lemma 2.6.** In the affine plane $\mathbb{A}^2(F_{q^2})$, the total number of non-vertical lines is $q^4$. Of these, $(q^4 - q^3)$ intersect $\mathcal{H}$ in $(q + 1)$ points and $q^3$ are tangent to $\mathcal{H}$, i.e. they intersect $\mathcal{H}$ in only one point.

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

$$\mathcal{H} \cap \mathcal{L} = \{(x, ax + b) \mid a^q x^q + b^q + ax + b = x^{q+1}, x \in F_{q^2}\}.$$ 

Let $c = c(a, b) = a^{q+1} + b^q + b$, then $c \in F_q$. 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 $c = (a^{q+1})^r$ for $1 \leq r \leq q - 1$, we have $x = a^q + \alpha^{r+1}(q-1)$ for any $0 \leq i \leq q$.

The number of pairs $(a, b)$ satisfying $c(a, b) = 0$ is $q^3$, because they correspond to the affine points of $\mathcal{H}'$, and those satisfying $c \neq 0$ are $(q^4 - q^3)$. \qed

**Corollary 2.7.** Let $\mathcal{L}$ be any horizontal line $\{y = b\}$, with $b \in F_{q^2}$. Then if $\text{Tr}(b) = 0$, $\mathcal{L}$ intersects $\mathcal{H}$ in one affine point, otherwise, if $\text{Tr}(b) \neq 0$, $\mathcal{L}$ intersects $\mathcal{H}$ in $q + 1$ affine points.
Proof. Apply Lemma 2.6 with \( a = 0 \). \( \square \)

3 Small-weight codewords of Hermitian Codes

We recall that an affine-variety code is \( \text{Im}(\phi(L)) \), where \( \phi \) is as (2). We consider a special case of affine-variety code, which is a Hermitian code.

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 \( B_{m,q} = \{ x^r y^s + I \mid qr + (q + 1)s \leq m, \ 0 \leq s \leq q - 1, \ 0 \leq r \leq q^2 - 1 \} \), where \( m \) is an integer such that \( 0 \leq m \leq q^3 + q^2 - q - 2 \). For simplicity, we also write \( x^r y^s \) for \( x^r y^s + I \). We consider the evaluation map \( (2) \phi : R \to (\mathbb{F}_{q^2})^n \).

We have the following affine–variety codes:

\[
C(I, L) = \text{Span}_{\mathbb{F}_{q^2}}(\phi(B_{m,q}))
\]

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 \( H \).

\[
H = \begin{pmatrix}
  f_1(P_1) & \ldots & f_1(P_n) \\
  \vdots & \ddots & \vdots \\
  f_i(P_1) & \ldots & f_i(P_n)
\end{pmatrix}
\]

where \( f_j \in B_{m,q} \).

The Hermitian codes can be divided in four phases ([HvLP98]), any of them having specific explicit formulas linking their dimension and their distance ([Mar13]), as in Table 1.

In the remainder of this paper we focus on the first phase. This case can be characterized by the condition \( d \leq q \).

3.1 Corner codes and edge codes

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

**Definition 3.1.** Let \( 2 \leq d \leq q \) and let \( 1 \leq j \leq d - 1 \).

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 \( B_{m,q} = L_0^d \sqcup \cdots \sqcup L_{d-2}^d \), then we say that \( C(m,q) \) is a corner code and we denote it by \( H_0^d \).
- If \( B_{m,q} = L_0^d \sqcup \cdots \sqcup L_{d-2}^d \sqcup \{ l_1^d, \ldots, l_j^d \} \), then we say that \( C(m,q) \) is an edge code and we denote it by \( H_j^d \).

From the formulas in Table 1 we have the following theorem.
### Table 1

The four “phases” of Hermitian codes

<table>
<thead>
<tr>
<th>Phase</th>
<th>m</th>
<th>Distance d</th>
<th>Dimension k</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>(0 \leq m \leq q^2 - 2)</td>
<td>(a + 1 \ a &gt; b) (a + 2 \ a = b) (\iff d \leq q)</td>
<td>(q^3 - \frac{a(a+1)}{2} - (b+1))</td>
</tr>
<tr>
<td></td>
<td>(m = aq + b)</td>
<td>(0 \leq b \leq a \leq q - 1)</td>
<td>(b \neq q - 1)</td>
</tr>
<tr>
<td>2</td>
<td>(q^2 - 1 \leq m \leq 4q - 3)</td>
<td>((q - a)q - q - b - 1 \ a \leq b)</td>
<td>(n - g - q^2 + aq + b + 2)</td>
</tr>
<tr>
<td></td>
<td>(m = 2q^2 - qa - q - b - 3)</td>
<td>((q - a)q \ a &gt; b)</td>
<td>(1 \leq a \leq q - 2)</td>
</tr>
<tr>
<td></td>
<td>(0 \leq b \leq q - 2)</td>
<td>(0 \leq b \leq q - 2)</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>(4q - 2 \leq m \leq n - 2)</td>
<td>(m - 2g + 2)</td>
<td>(n - m + g - 1)</td>
</tr>
<tr>
<td>4</td>
<td>(n - 1 \leq m \leq n + 2g - 2)</td>
<td>(n - aq - b)</td>
<td>(\frac{a(a+1)}{2} + b + 1)</td>
</tr>
<tr>
<td></td>
<td>(m = n + 2g - 2 - aq - b)</td>
<td>(0 \leq b \leq a \leq q - 2),</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Theorem 3.2.** Let \(2 \leq d \leq q\), \(1 \leq j \leq d - 1\). Then

\[
d(H_d^0) = d(H_d^1) = d, \quad \dim_{F_{q^2}}(H_d^0) = n - \frac{d(d - 1)}{2}, \quad \dim_{F_{q^2}}(H_d^1) = n - \frac{d(d - 1)}{2} - j
\]

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 \(q \geq 3\)).

- **\(H_2^0\)** is a \([n, n - 1, 2]\) code.
  - \(B_{m,q} = L_0^2 \cup \{1\}\), so the parity-check matrix of \(H_2^0\) is \((1, \ldots, 1)\).

- **\(H_2^1\)** is a \([n, n - 2, 2]\) code.
  - \(B_{m,q} = L_0^2 \cup \{1, x\}\)

- **\(H_3^0\)** is a \([n, n - 3, 3]\) code.
  - \(B_{m,q} = L_0^3 \cup L_1^3 = \{1, x, y\}\)

- **\(H_3^1\)** is a \([n, n - 4, 3]\) code.
  - \(B_{m,q} = L_0^3 \cup L_1^3 \cup \{l^3_1, l^3_2\} = \{1, x, y, x^2\}\)

- **\(H_3^2\)** is a \([n, n - 5, 3]\) code.
  - \(B_{m,q} = L_0^3 \cup L_1^3 \cup \{l^3_1, l^3_2\} = \{1, x, y, x^2, xy\}\)
3.2 First results for the first phase

Ideal $J_w$ of Proposition 2.2 for $C(m, q)$ is

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

Let $w \geq v \geq 1$. Let $Q = (x_1, \ldots, x_w, y_1, \ldots, y_w, z_1, \ldots, z_w) \in \mathcal{V}(J_w)$. 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

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

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

Lemma 3.3. 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 $u + v \leq \lfloor \frac{w}{2} \rfloor + 2$.

We need the following technical lemma [Pel,Mar13].

Lemma 3.4. Let us consider the edge code $H_d^j$ with $1 \leq j \leq d - 1$ and $3 \leq d \leq w \leq 2d - 3$. Let $Q = (x_1, \ldots, x_w, y_1, \ldots, y_w, z_1, \ldots, z_w)$ be a solution of $J_w$ in $v$-block position, with $v \leq w$, then exactly one of the following cases holds:

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

or

(b) $v = 1$, that is, $\overline{x}_1 = \cdots = \overline{x}_w$.

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

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

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

(a) $u = 1$. We have to prove, by contradiction, that $v > d$.

Let $v \leq d$. Since $Q \in \mathcal{V}(J_w)$, then $L_w^0(Q) = L_1^w(Q) = 0$, that is

$$0 = \sum_{i=1}^{w} \overline{x}_i^r \overline{z}_i = \sum_{i \in I_h} X_h^r \overline{z}_i = \sum_{h=1}^{v} X_h^r Z_h \quad 0 \leq r \leq d - 1. \quad (10)$$
We only need to consider only the first $v$ equations of (10), because $v \leq d$, so
\[ \sum_{h=1}^{v} X_h^r Z_h = 0 \]
where $0 \leq r \leq v - 1$, that is,
\[
\begin{pmatrix}
1 & \ldots & 1 \\
X_1 & \ldots & X_v \\
\vdots & \ldots & \vdots \\
X_1^{v-1} & \ldots & X_v^{v-1}
\end{pmatrix}
\begin{pmatrix}
Z_1 \\
\vdots \\
Z_v
\end{pmatrix}
= 0
\] (11)

The above matrix is a Vandermonde matrix, so it has maximal rank $v$. Therefore, the solution of (11) is $(Z_1, \ldots, Z_v) = (0, \ldots, 0)$. Since $u = 1$, then $Z_1 = \bar{y}_1 = 0$, 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 2.2. A subset of equations of condition (4) is the following system, where $0 \leq r \leq v$
\[
\begin{cases}
\sum_{i=1}^{u} \bar{x}_i^r \bar{z}_i = 0 \\
\sum_{i=1}^{w} \bar{x}_i^r \bar{y}_i \bar{z}_i = 0 \\
\vdots \\
\sum_{i=1}^{w} \bar{x}_i^r \bar{y}_i^{u-1} \bar{z}_i = 0
\end{cases}
\iff
\begin{cases}
\sum_{h=1}^{v} X_h^r Z_h = 0 \\
\sum_{h=1}^{v} X_h^r Y_{h,1} = 0 \\
\vdots \\
\sum_{h=1}^{v} X_h^r Y_{h,u-1} = 0
\end{cases}
\] (12)

In fact system (12) is a subset of (4) if and only if
\[ \deg(\bar{x}_i^r \bar{y}_i^{u-1}) \leq d - 1 \]
for any $i = 1, \ldots, w$. 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 3.3 and we obtain
\[ u + v \leq \left\lceil \frac{w}{2} \right\rceil + 2 \leq \left\lceil \frac{2d-3}{2} \right\rceil + 2 = d. \]

By system (12) we obtain $u$ Vandermonde matrices (all having rank $v$). Therefore, the solutions of these systems are zero-solutions. So, in the particular case $h = 1$, we have $Z_1 = Y_{1,1} = \ldots = Y_{1,u-1} = 0$, that is
\[
\begin{cases}
\sum_{i=0}^{u} \bar{z}_i = 0 \\
\sum_{i=0}^{u} \bar{y}_i \bar{z}_i = 0 \\
\vdots \\
\sum_{i=0}^{u} \bar{y}_i^{u-1} \bar{z}_i = 0
\end{cases}
\iff
\begin{pmatrix}
1 & \ldots & 1 \\
\bar{y}_1 & \ldots & \bar{y}_u \\
\vdots & \ldots & \vdots \\
\bar{y}_1^{u-1} & \ldots & \bar{y}_u^{u-1}
\end{pmatrix}
\begin{pmatrix}
\bar{z}_1 \\
\vdots \\
\bar{z}_u
\end{pmatrix}
= 0
\]

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 $\bar{z}_1 = \cdots = \bar{z}_u = 0$, but this is impossible because $\bar{z}_i \in \mathbb{F}_{q^2} \setminus \{0\}$. Therefore $v = 1$.

The case $H_2^1$ is trivial. \qed
3.3 Minimum-weight codewords

Corollary 3.5. Let us consider the edge code $H^d_j$ with $1 \leq j \leq d - 1$.

If $Q = (\bar{x}_1, \ldots, \bar{x}_d, \bar{y}_1, \ldots, \bar{y}_d, \bar{z}_1, \ldots, \bar{z}_d) \in \mathcal{V}(J_d)$, 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 $H$ and a vertical line.

Whereas if $d \geq 4$ and $Q = (\bar{x}_1, \ldots, \bar{x}_{d+1}, \bar{y}_1, \ldots, \bar{y}_{d+1}, \bar{z}_1, \ldots, \bar{z}_{d+1}) \in \mathcal{V}(J_{d+1})$, then one of the following cases holds

(a) $\bar{x}_i \neq \bar{x}_j$ with $i \neq j$ for $1 \leq i, j \leq d + 1$.

or

(b) $\bar{x}_1 = \cdots = \bar{x}_{d+1}$.

Proof. We are in the hypotheses of Lemma 3.4. 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 3.4, 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 for edge codes.

Theorem 3.6. 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 2.2 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:

$$\begin{align*}
\bar{z}_1 + \cdots + \bar{z}_d &= 0 \\
\bar{x}_1 \bar{z}_1 + \cdots + \bar{x}_d \bar{z}_d &= 0 \\
\bar{y}_1 \bar{z}_1 + \cdots + \bar{y}_d \bar{z}_d &= 0 \\
&\vdots \\
\bar{y}_1^{d-2} \bar{z}_1 + \cdots + \bar{y}_d^{d-2} \bar{z}_d &= 0 \\
\bar{x}_1^{d-1} \bar{z}_1 + \cdots + \bar{x}_d^{d-1} \bar{z}_d &= 0
\end{align*}$$

(13)

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

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

(14)
But \( \bar{x}_1 \ldots = \bar{x}_d \), since we are in the hypotheses of Corollary 3.5. So the system becomes

\[
\begin{align*}
\bar{z}_1 + \cdots + \bar{z}_d &= 0 \\
\bar{y}_1 \bar{z}_1 + \cdots + \bar{y}_d \bar{z}_d &= 0 \\
&\vdots \\
\bar{y}_1^{d-2} \bar{z}_1 + \cdots + \bar{y}_d^{d-2} \bar{z}_d &= 0
\end{align*}
\]

We have \( q^2 \) choices for the \( \bar{x}_i \)'s and, by Lemma 2.5, we have \( \binom{q}{d} \) different \( \bar{y}_i \)'s, since for any choice of the \( \bar{x}_i \)'s there are exactly \( q \) possible values 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 compute the solutions for the \( \bar{z}_i \)'s.

We write the system (15) 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 \( \alpha \in \mathbb{F}_{q^2}^\ast \), where \( a_j \) are fixed since they depend on \( \bar{y}_i \). So the number of the \( z \)'s is \( |\mathbb{F}_{q^2}^\ast| = q^2 - 1 \), then \( A_d = \frac{1}{d!} \left( q^2(q^2 - 1)\binom{q}{d} d! \right) \). □

We consider now corner codes. We have the following geometric characterisation.

**Proposition 3.7.** Let us consider the corner code \( \mathcal{H}_d^1 \). 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,

\[
\begin{align*}
\bar{z}_1 + \cdots + \bar{z}_d &= 0 \\
\bar{x}_1 \bar{z}_1 + \cdots + \bar{x}_d \bar{z}_d &= 0 \\
\bar{y}_1 \bar{z}_1 + \cdots + \bar{y}_d \bar{z}_d &= 0 \\
&\vdots \\
\bar{y}_1^{d-2} \bar{z}_1 + \cdots + \bar{y}_d^{d-2} \bar{z}_d &= 0
\end{align*}
\]

This system is the same as (13), but with a missing equation. This means that (16) has all solutions of system (13) and other solutions. If we consider a subset of (16), which has just the variables \( x \)'s and \( z \)'s, 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 (16) and we exchange \( x \) with \( y \), we obtain again (16). So we have two alternatives:
• 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 will prove that they lie on a non-horizontal line that intersects the Hermitian curve.

Let $y = \beta x + \lambda$ be a non-vertical line passing through 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 at least two of the $y'$’s are equal and not all $y$’s are coincident.

Substituting the above transformation in (16) and applying some operations between the equations, we obtain a system that is equivalent to (16). But this new system has 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.

\[\square\]

We finally prove the following theorem:

**Theorem 3.8.** The number of words having weight $d$ of a corner code $H_0^d$ is

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

**Proof.** Again, the points corresponding to minimum-weight words of a corner code have to verify (16). By above proposition, we know that these points lie in the intersections of any line and the Hermitian curve $H$.

Let $Q = (\bar{x}_1, \ldots, \bar{x}_d, \bar{y}_1, \ldots, \bar{y}_d, \bar{z}_1, \ldots, \bar{z}_d) \in \mathcal{V}(J_d)$ such that $\bar{x}_1 = \ldots = \bar{x}_d$, 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

$$q^2(q^2 - 1)\left(\frac{q}{d}\right)d!.$$  

Now we have to compute 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 2.6 we know that the number of the $\bar{y}_i$’s and $\bar{x}_i$’s is

$$(q^4 - q^3)\left(\frac{q + 1}{d}\right)d!,$$

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 these (and the system is invariant). As regards the number of the $\bar{z}_i$’s, we have to compute the number of solutions of system (16).

We apply an affine transformation to the system (16) to obtain a horizontal line, that is, to have all the $\bar{x}_i$’s different and all the $\bar{y}_i$’s equal, so we obtain a system equivalent to system (15). Therefore we have a Vandermonde matrix,
hence the number of the $z_i$’s is $q^2 - 1$. So

$$A_d = \frac{1}{d!} \left( q^2(q^2 - 1)\left(\begin{array}{c} q \\ d \end{array}\right) + (q^4 - q^3)(q^2 - 1)\left(\begin{array}{c} q+1 \\ d+1 \end{array}\right) \right) = q^2(q^2 - 1)\left(\begin{array}{c} q \\ d+1 \end{array}\right) \frac{q^2 - d+1}{d}.$$ 

\[\square\]

### 3.4 Second-weight codewords

In this section we state more theorems for edge and corner codes previously consider in [Mar08,Mar13]. We study the case when the $x_i$’s coincide or when the $y_i$’s coincide.

**Theorem 3.9.** The number of words of weight $d + 1$ with $y_1 = \ldots = y_{d+1}$ of a corner code $H^0_0$ is:

$$(q^2 - q)(q^4 - (d+1)q^2 + d)\left(\begin{array}{c} q+1 \\ d+1 \end{array}\right).$$

Whereas for an edge code $H^0_j$ with $1 \leq j \leq d - 1$ the numbers is:

$$(q^2 - q)\left(\begin{array}{c} q+1 \\ d+1 \end{array}\right).$$

**Proof.** We have $q^2$ choice for the $y_i$’s and, by Corollary 2.7, we have $(q^2 - 1)\left(\begin{array}{c} q+1 \\ d+1 \end{array}\right)!$ different $x_i$’s, since for any choice of the $y_i$’s there are exactly $q + 1$ possible values for the $x_i$’s, but we need just $(d + 1)$ of them and any permutation of these will be again a solution. Now we have to compute the solutions for the $z_i$’s, in the two distinct cases.

* Case $H^0_0$. By Proposition 2.2 we know that $J_d$ represents all words of minimum weight. The first set of ideal basis (9) has exactly $\left(\begin{array}{c} d \end{array}\right)$ equations, which is system (16) with more variables, that is, instead of $\bar{x}_d$, $\bar{y}_d$ and $\bar{z}_d$, we have, respectively, $\bar{x}_{d+1}$, $\bar{y}_{d+1}$ and $\bar{z}_{d+1}$. Since $\bar{y}_1 = \ldots = \bar{y}_{d+1}$, the said variation of system (16) is

$$\begin{aligned}
\bar{z}_1 + \cdots + \bar{z}_{d+1} &= 0 \\
\bar{x}_1 \bar{z}_1 + \cdots + \bar{x}_{d+1} \bar{z}_{d+1} &= 0 \\
&\vdots \\
\bar{x}^{d-2}_1 \bar{z}_1 + \cdots + \bar{x}^{d-2}_{d+1} \bar{z}_{d+1} &= 0 
\end{aligned} \tag{17}$$

We can note that, if we write the system (17) as a matrix adding these two equations $x_1^{d-1} + \cdots + x_{d+1}^{d-1} = 0$ and $x_1^d + \cdots + x_{d+1}^d = 0$ we obtain a Vandermonde matrix. So all rows of (17) are linearly independent. This means that the solution space has linear dimension 2 because $2 = (d+1) - (d-1)$. So the number of the $z$’s is $q^2 - \left|\{z_i = 0 \text{ for at least an } i\}\right|$, since we have...
\( q^2 \) for each \( z_{d+1} \) and \( z_d \). We want to compute the number of \( z_i = 0 \) for at least one \( i \).

Since the matrix \( H \) has maximum rank, we can apply the Gauss elimination to the system (17)

\[
\begin{align*}
\bar{z}_1 + \cdots + \bar{z}_{d+1} &= 0 \\
h_{2,2} \bar{z}_2 + \cdots + h_{2,d} \bar{z}_d + h_{2,d+1} + \bar{z}_{d+1} &= 0 \\
\vdots \\
h_{d-1,d-2} \bar{z}_{d-2} + h_{d-1,d-1} \bar{z}_{d-1} + h_{d-1,d} \bar{z}_d + h_{d-1,d+1} \bar{z}_{d+1} &= 0 \\
h_{d-1,d-1} \bar{z}_{d-1} + h_{d-1,d} \bar{z}_d + h_{d-1,d+1} \bar{z}_{d+1} &= 0
\end{align*}
\]

(18)

If we solve the system (18) we obtain

\[
h_{d-1,d-1} \bar{z}_{d-1} + h_{d-1,d} \bar{z}_d + h_{d-1,d+1} \bar{z}_{d+1} = 0
\]

(19)

First of all we consider the case \( \bar{z}_{d-1} = 0 \), that is

\[
h_{d-1,d} \bar{z}_d + h_{d-1,d+1} \bar{z}_{d+1} = 0 \iff \bar{z}_d = -\frac{h_{d-1,d+1}}{h_{d-1,d}} \bar{z}_{d+1}
\]

(20)

The equation (20) in the variable \( \bar{z}_{d+1} \in \mathbb{F}_{q^2} \) has exactly \( q^2 \) solutions. In particular, we have the pair \((\bar{z}_d, \bar{z}_{d+1}) = (0, 0)\) and other \( q^2 - 1 \) ways to choose the variable \( \bar{z}_{d+1} \).

We have similar conditions when \( \bar{z}_d = 0 \) and \( \bar{z}_{d+1} = 0 \). As before we have the pairs \((\bar{z}_{d-1}, \bar{z}_{d+1}) = (0, 0)\) and \((\bar{z}_{d-1}, \bar{z}_d) = (0, 0)\) and other \( q^2 - 1 \) ways to choose \( \bar{z}_{d-1} \) and \( q^2 - 1 \) ways to choose \( \bar{z}_d \).

So the equation (19) has exactly \( 3(q^2-1) + |\{(\bar{z}_{d-1}, \bar{z}_d, \bar{z}_{d+1}) = (0, 0, 0)\}| = 3q^2 - 2 \) solutions.

Now we consider the second last line of the system (18): \( h_{d-1,d-2} \bar{z}_{d-2} + h_{d-1,d-1} \bar{z}_{d-1} + h_{d-1,d} \bar{z}_d + h_{d-1,d+1} \bar{z}_{d+1} = 0 \), that is,

\[
\bar{z}_{d-2} = -(k_{d-1} \bar{z}_{d-1} + k_d \bar{z}_d + k_{d+1} \bar{z}_{d+1})
\]

(21)

First of all we have to study the case \( \bar{z}_{d-2} = 0 \). We just studied the case in which all variables \( \bar{z}_{d-1} = \bar{z}_d = \bar{z}_{d+1} = 0 \), so we have to study the case when all variables are different from zero, that is, \( \frac{k_{d-1}}{k_{d+1}} \bar{z}_{d-1} + \frac{k_d}{k_{d+1}} \bar{z}_d = -\bar{z}_{d+1} = k \in \mathbb{F}_{q^2}^* \). So the equation (21) has exactly \( (q^2-1) \) solutions.

We repeat the argument for each of system’s equations (18), there are \( (d-2) \) of them, if we do not count the last equation. Therefore

\[
\#(\bar{z}_i = 0 \text{ for at least one } i) = 3q^2 - 2 + (d - 2)(q^2 - 1) = (d + 1)q - d
\]

So the system (18) has exactly \( q^4 - (d + 1)q + d \) solutions. Then the
number of words of weight \(d + 1\) with \(y_1 = \ldots = y_{d+1}\) of \(H_d^0\) is:

\[
(q^2 - q)(q^4 - (d + 1)q^2 + d)\binom{q + 1}{d + 1}.
\]

**Case** \(H_d^j\). In this case the first set of ideal basis (9) contains exactly \(d(d-1)/2 + j\) equations, where \(1 \leq j \leq d - 1\). So, if \(j = 1\), this set implies the system (13) with more variables, that is, instead of \(\bar{x}_d, \bar{y}_d\) and \(\bar{z}_d\), we have, respectively, \(\bar{x}_{d+1}, \bar{y}_{d+1}\) and \(\bar{z}_{d+1}\). Whereas, if \(j > 1\) then we have to add the first \(j - 1\) of equations (14) with more variables.

Since \(\bar{y}_1 = \ldots = \bar{y}_{d+1}\), the system becomes

\[
\begin{align*}
\bar{z}_1 + \cdots + \bar{z}_{d+1} &= 0 \\
\bar{x}_1\bar{z}_1 + \cdots + \bar{x}_{d+1}\bar{z}_{d+1} &= 0 \\
&\vdots \\
\bar{x}_1^{d-1}\bar{z}_1 + \cdots + \bar{x}_{d+1}^{d-1}\bar{z}_{d+1} &= 0
\end{align*}
\tag{22}
\]

This means that the solution space has linear dimension \(d - (d - 1) = 1\). So the number of the \(z\)'s is \(|F_{q^2}^d| = q^2 - 1\), then the number of words of weight \(d + 1\) with \(y_1 = \ldots = y_{d+1}\) of \(H_d^j\) is

\[
(q^2 - 1)(q^2 - q)\binom{q + 1}{d + 1}.
\]

\[\square\]

**Theorem 3.10.** 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:

\[
q^2(q^4 - (d + 1)q^2 + d)\binom{q}{d + 1}.
\]

**Proof.** By Proposition 2.2 we know that \(J_d\) represents all words of minimum weight. For an edge code the first set of ideal basis (9) implies, if \(j = 1\) the system (13) with more variables\(^1\) and if \(j > 1\) we have to add the first \(j - 1\) of equations (14) with more variables. Whereas, for a corner code, the first set of ideal basis (9) implies the system (16) with more variables. But

\(^1\) instead of \(\bar{x}_d, \bar{y}_d\) and \(\bar{z}_d\), we have, respectively, \(\bar{x}_{d+1}, \bar{y}_{d+1}\) and \(\bar{z}_{d+1}\). This is true every time that we write with more variables.
The systems becomes

\[
\begin{align*}
\bar{z}_1 + \cdots + \bar{z}_{d+1} &= 0 \\
\bar{y}_1 \bar{z}_1 + \cdots + \bar{y}_{d+1} \bar{z}_{d+1} &= 0 \\
&\vdots \\
\bar{y}_1^{d-2} \bar{z}_1 + \cdots + \bar{y}_1^{d-2} \bar{z}_{d+1} &= 0
\end{align*}
\]

(23)

We have \(q^2\) choice for the \(\bar{x}_i\)’s and, by Lemma 2.5, we have \(\binom{q}{d+1}(d+1)!\) different \(\bar{y}_i\)’s, since for any choice of the \(\bar{x}_i\)’s there are exactly \(q\) possible values for the \(\bar{y}_i\)’s, but we need just \(d+1\) of them and any permutation of these will be again a solution. And we have \((q^4 - (d+1)q^2 + d)\) possible \(\bar{z}_i\)’s which is exactly the situation met in Theorem 3.9.

\[\square\]

**Theorem 3.11.** The number of words of weight \(d+1\) of a corner code \(H^0_d\) with \((x_i, y_i)\) lying on a non-vertical line is:

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

**Theorem 3.12.** The number of words of weight \(d+1\) of an edge code \(H^1_d\) with \((x_i, y_i)\) lying on a non-vertical line is:

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

The proofs are similar to those of the statements as in Section 3.2 and the previous theorems and so are omitted.

In other cases, we have to consider the intersection of the curve with higher degree curves and the formulas get more complicated. For example the cubic found in [Cou11,BR12a].

Now we are going to study some special cases of Hermitian codes, that is, we count the number of words having weight \(d+1\) for any Hermitian code having distance \(d = 3\) or \(d = 4\). In the following section we are going to prove these theorems:

**Theorem 3.13.** The number of words of weight 4 of a corner code \(H^0_3\) is:

\[A_4 = \frac{1}{4} \left( \binom{q^3}{3} (q+1) - q^2 \binom{q+1}{3} (3q^3 + 2q^2 - 8) \right) (q-1)(q^3 - 3).

The number of words of weight 4 of an edge code \(H^1_3\) is:

\[A_4 = q^2 \binom{q}{4} (q^4 - 4q^2 + 3) + \frac{q^4(q^2 - 1)^2(q-1)^2}{8} + (q^2 - 1) \sum_{k=4}^{2d} N_k \binom{k}{4}.
\]
Where $N_k$ is the number of parabolas and non-vertical lines that intersect $H$ in exactly $k$ points.

The number of words of weight 4 of an edge code $H_3^2$ is:

$$A_4 = q^2(q-1)\left(\frac{q+1}{4}\right)(2q^3 - 3q^2 - 4q + 9).$$

**Theorem 3.14.** The number of words of weight 5 of a corner code $H_4^0$ is:

$$A_5 = \frac{1}{5}q^2\binom{q}{4}(q^3 - 4)(q^2 - 1)(q^2 - 4).$$

The number of words of weight 5 of all edge codes $H_j^4$ for $1 \leq j \leq 3$ is:

$$A_5 = q^2(q-1)\left(\frac{q+1}{5}\right)(2q^3 - 4q^2 - 5q + 16).$$

The formula for $A_4$ of $H_3^1$ in Theorem 3.13 contains some implicit values $N_k$'s. To derive explicit values it is enough to consider Theorem 3.1 of [MPS12].

### 3.5 The complete investigation for $d = 3, 4$.

In this section we will study separately the corner and edge codes of distance 3 and 4, that is, $H_0^3, H_1^3, H_2^3, H_4^0, \{H_j^4\}_{1 \leq j \leq 3}$.

**Study of $H_3^0$.**

Now we count the number of words with weight $w = 4$. In this case, the first condition set of $J_w$ becomes:

\[
\begin{align*}
z_1 + z_2 + z_3 + z_4 &= 0 \\
x_1z_1 + x_2z_2 + x_3z_3 + x_4z_4 &= 0 \\
y_1z_1 + y_2z_2 + y_3z_3 + y_4z_4 &= 0
\end{align*}
\]

We notice that this is a linear system in $z_i$. We first choose 4 points $P_i = (x_i, y_i)$ on $H$ and then we compute the number of solutions in $z_i$'s. The coefficient matrix is

\[
\begin{pmatrix}
1 & 1 & 1 & 1 \\
x_1 & x_2 & x_3 & x_4 \\
y_1 & y_2 & y_3 & y_4
\end{pmatrix}
\]

This matrix cannot have rank 1. If the rank is 2, this means that all $P_i$'s lie on a same line. The vector space of solutions has dimension 2, so that we have $q^4 - 4(q^2 - 1) - 1$ solutions in $z_i$'s (we have to exclude the zero solution and solutions with one $z_i = 0$).

Otherwise, the rank is 3. In this case, we have 3 points on a same line, say $P_1, P_2, P_3$, if and only if we have a square submatrix of order 3 whose
determinant is 0, but this implies that \( z_4 = 0 \), which is not admissible. If we choose 4 points such that no 3 of them lie on a same line, all \( z_i \)'s will be non-zero and we get a codeword. The vector space of solutions has dimension 1, so that we have \( q^2 - 1 \) solutions in \( z_i \)'s (we have to exclude the zero solution).

If the rank is 2, the total number of solutions (in \( x_i, y_i, z_i \)) is

\[
\left( q^2 \left( \frac{q}{4} \right) + (q^4 - q^3) \left( \frac{q + 1}{4} \right) \right) (q^4 - 4q^2 + 3).
\]

If the rank is 3, the total number of solutions (in \( x_i, y_i, z_i \)) is

\[
\left( \frac{q^3}{4} - q^2 \left( \frac{q}{3} \right) (q^3 - q) - (q^4 - q^3) \left( \frac{q + 1}{3} \right) (q^3 - q - 1) + q^2 \left( \frac{q}{4} \right) - (q^4 - q^3) \left( \frac{q + 1}{4} \right) \right) (q^2 - 1).
\]

Putting together, we get the total number of codewords of weight 4 of \( H_0^3 \):

\[
A_4 = \left( \frac{q^3}{4} - q^2 \left( \frac{q}{3} \right) (q^3 - q) - (q^4 - q^3) \left( \frac{q + 1}{3} \right) (q^3 - q - 1) \right) (q^2 - 1) + \\
+ \left( q^2 \left( \frac{q}{4} \right) + (q^4 - q^3) \left( \frac{q + 1}{4} \right) \right) (q^4 - 5q^2 + 4).
\]

Doing the computations we obtain the first part of Theorem 3.13.

**Study of \( H_1^3 \).**

We count the number of words with weight \( w = 4 \). In this case, the first condition set of \( J_w \) becomes:

\[
\begin{align*}
& z_1 + z_2 + z_3 + z_4 = 0 \\
& x_1 z_1 + x_2 z_2 + x_3 z_3 + x_4 z_4 = 0 \\
& y_1 z_1 + y_2 z_2 + y_3 z_3 + y_4 z_4 = 0 \\
& x_1^2 z_1 + x_2^2 z_2 + x_3^2 z_3 + x_4^2 z_4 = 0
\end{align*}
\]

As above, we first choose 4 points \( P_i = (x_i, y_i) \) on \( \mathcal{H} \) and then we compute the number of solutions in \( z_i \)'s. The coefficient matrix is

\[
\begin{pmatrix}
1 & 1 & 1 & 1 \\
x_1 & x_2 & x_3 & x_4 \\
y_1 & y_2 & y_3 & y_4 \\
x_1^2 & x_2^2 & x_3^2 & x_4^2
\end{pmatrix}
\]

Now we study the rank of the matrix according to “v-blocks”.

---

CGC
If all $x_i$'s are equal, we have 4 points on a vertical line; the rank is 2 (see below) and the number of codewords is (see case $H^0_3$)

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

If only three $x_i$'s are equal, we have 3 points on a vertical line and another one outside, but this configuration is impossible for $H^0_3$ (that is, we do not have codewords associated to it), and it is also impossible for $H^1_3$, since $H^1_3 \subset H^0_3$.

If we have two pairs of equal $x_i$'s (for instance, $x_1 = x_2 \neq x_3 = x_4$), we can have codewords. In this case, we deduce $z_1 + z_2 = 0$, $z_3 + z_4 = 0$, $z_1(y_1 - y_2) + z_3(y_3 - y_4) = 0$, so that we have $\binom{q^2}{2}$ ways to choose $\{x_1, x_3\}$, $\binom{q}{2}$ ways to choose $\{y_1, y_2\}$, $\binom{q}{2}$ ways to choose $\{y_3, y_4\}$, $q^2 - 1$ ways to choose $z_1$, this determines all $z_i$. The number of codewords in this case is

$$\frac{q^4(q^2 - 1)^2(q - 1)^2}{8}.$$

If only two $x_i$'s are equal, say $x_1 = x_2$, we can show that we have $z_1 + z_2 = 0$, $z_3 = 0$, $z_4 = 0$, which is not admissible.

If we have all $x_i$'s distinct, the submatrix

$$\begin{pmatrix}
1 & 1 & 1 & 1 \\
x_1 & x_2 & x_3 & x_4 \\
x_1^2 & x_2^2 & x_3^2 & x_4^2
\end{pmatrix}$$

has rank 3, but if the whole matrix (24) has rank 4 we can only have the zero solution, which is not admissible. Thus, (24) must have rank 3, that is, the $y_i$'s row must be linearly dependent on the other rows. This means that

$$\exists a, b, c \in \mathbb{F}_{q^2} \text{ such that } y_i = ax_i^2 + bx_i + c \forall i = 1, \ldots, 4.$$  

That is, all $P_i$'s lie on the same parabola (or on the same non-vertical line, when $a = 0$). In this case, the number of codewords is

$$(q^2 - 1) \sum_{k=4}^{2q} N_k \binom{k}{4},$$

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

Putting all together we get $A_4$, that is, the second part of Theorem 3.13.

**Study of $H^2_3$.**

We count the number of words with weight $w = 4$. In this case, the first
condition set of $J_w$ becomes:

\[
\begin{aligned}
&z_1 + z_2 + z_3 + z_4 = 0 \\
x_1z_1 + x_2z_2 + x_3z_3 + x_4z_4 = 0 \\
y_1z_1 + y_2z_2 + y_3z_3 + y_4z_4 = 0 \\
x_1^2z_1 + x_2^2z_2 + x_3^2z_3 + x_4^2z_4 = 0 \\
x_1y_1z_1 + x_2y_2z_2 + x_3y_3z_3 + x_4y_4z_4 = 0
\end{aligned}
\]

As above, we first choose 4 points $P_i = (x_i, y_i)$ on $\mathcal{H}$ and then we compute the number of solutions in $z_i$'s. The coefficient matrix is

\[
\begin{pmatrix}
1 & 1 & 1 & 1 \\
x_1 & x_2 & x_3 & x_4 \\
y_1 & y_2 & y_3 & y_4 \\
x_1^2 & x_2^2 & x_3^2 & x_4^2 \\
x_1y_1 & x_2y_2 & x_3y_3 & x_4y_4
\end{pmatrix}
\]

Now we study the rank of the matrix according to “v-blocks”.

If all $x_i$’s are equal, we have 4 points on a vertical line; the rank is 2 (see below) and the number of codewords is (see case $H_3^1$)

\[
q^2\binom{q}{4}(q^4 - 4q^2 + 3).
\]

If only three $x_i$’s are equal, we have 3 points on a vertical line and another one outside, but this configuration is impossible (as above).

If we have two pairs of equal $x_i$’s (for instance, $x_1 = x_2 \neq x_3 = x_4$), we can deduce $z_1 + z_2 = 0, z_3 + z_4 = 0$, and then

\[
\begin{aligned}
z_1(y_1 - y_2) + z_3(y_3 - y_4) &= 0 \\
x_1z_1(y_1 - y_2) + x_3z_3(y_3 - y_4) &= 0
\end{aligned}
\]

but this system in the unknowns $y_1 - y_2, y_3 - y_4$ has determinant $z_1z_3(x_3 - x_1) \neq 0$, so that $y_1 = y_2$, which is impossible.

If only two $x_i$’s are equal, say $x_1 = x_2$, we can show that we have $z_1 + z_2 = 0, z_3 = 0, z_4 = 0$, which is not admissible.

If we have all $x_i$’s distinct, the submatrix

\[
\begin{pmatrix}
1 & 1 & 1 & 1 \\
x_1 & x_2 & x_3 & x_4 \\
x_1^2 & x_2^2 & x_3^2 & x_4^2
\end{pmatrix}
\]
has rank 3, but if the whole matrix (25) has rank 4 we can only have the zero solution, which is not admissible. Thus, (25) must have rank 3, that is, the $y_i$’s and $x_i y_i$’s rows must be linearly dependent on the other rows. This means that $y = ax^2 + bx + c$ and $xy = dx^2 + ex + f$, then $ax^3 + (b - d)x^2 + (c - e)x - f = 0$. But this equation can have at most 3 distinct solutions, and we need 4. Thus we must have $a = 0, b = d, c = e, f = 0$, that is, $y = bx + c$: all $P_i$’s lie on a same non-vertical line, and the number of codewords is

\[(q^4 - q^3)\left(\frac{q + 1}{5}\right)(q^2 - 1)\]

Putting all together we get $A_4$, that is, the last part of Theorem 3.13.

**Study of $H_0^4$.**

We count the number of words with weight $w = 5$. We have a linear system in $z_i$ with a $(6 \times 5)$ matrix. If its rank is 5, we can only have the zero solution, which is not admissible. Thus, its rank must be at most 4; this means that we have at least 2 relationships of linear dependency, say

\[
\begin{align*}
xy &= a + bx + cy + dx^2 \\
y^2 &= e + fx + gy + hx^2.
\end{align*}
\]

We need to find 5 points on the intersection of 2 different conics, but this means that the 2 conics must be degenerate, they must have a common line, and all 5 points belong to this line. We could distinguish between vertical lines and non-vertical lines, but in both cases the rank of the matrix is exactly 3. So, the number of codewords is

\[A_5 = \left(\left(q^4 - q^3\right)\left(\frac{q + 1}{5}\right) + q^2\left(\frac{q}{5}\right)\right)(q^4 - 5q^2 + 4)\]

Doing the computations we obtain the first part of Theorem 3.14.

**Study of $H_1^4$, $H_2^4$, $H_3^4$.**

To count the number of words with weight $w = 5$, we remember that

\[H_0^4 \supseteq H_1^4 \supseteq H_2^4 \supseteq H_3^4 \supseteq H_0^0\]

and the first and the last code have all words with weight 5 corresponding to 5 points on a line. We notice that for a vertical line the rank of the matrix is 3, while for a non-vertical line the rank of the matrix is 4. So, the number of codewords is

\[A_5 = q^2\left(\frac{q}{5}\right)(q^4 - 5q^2 + 4) + \left(q^4 - q^3\right)\left(\frac{q + 1}{5}\right)(q^2 - 1)\]

Doing the computations we obtain the last part of Theorem 3.14.
4 Conclusions and open problems

The so-called first-phase codes have nice geometric properties that allow their study, as first realized in [Pel06] and [SP06]. In particular, the fact that all minimum-weight codewords lie on intersections of lines and $\mathcal{H}$ is essential. Recent research has widened this approach to intersection with degree-2 and degree-3 curves [Cou11,BR12b], unfortunately without reaching an exact formula for higher weights. We believe that only complete classifications of intersections of $\mathcal{H}$ and higher degree curves can lead to the determination of the full weight distribution of first-phase Hermitian codes. We invite the reader to pursue this approach further.

As regards the other phases, it seems that only a part of the second phase can be described in a similar way. Therefore, probably a radically different approach is needed for phase-3, 4 codes in order to determine their weight distribution completely. Alas, we have no suggestions as to how reach this.

Acknowledgements

This work was partially presented in 2006 at two conferences: [Pel06] and [SP06], in 2010 at the Claude Shannon Institute WCC, Cork (Ireland), in 2011 at the Mzuni Math Workshop, Mzuzu University (Malawi) and at WCC 2011 [PMS11].

The seminal idea behind our starting point (Proposition 2.2) was in the second author’s PhD thesis [Pel], which was studied in deep and generalized in the first author Master’s thesis and PhD thesis [Mar08,Mar13]. The first two authors would like to thank their supervisor, the third author.

The authors would like to thank C. Traverso for seminal discussions in 2005 on the relation between small-weight codewords and variety points.

We have run our computer simulations using the software package Singular and MAGMA [GPS07,MAG] and all our programmes and their digital certificates are available under request.

References


M. Sala and M. Pellegrini, The number of minimum weight words for any Hermitian code with $d \leq q$, Third Workshop on Coding and Systems, Zurich (2006).