Journal of Symbolic Computation 73 (2016) 27–45

Contents lists available at ScienceDirect

Journal of Symbolic Computation

www.elsevier.com/locate/jsc

On the small-weight codewords of some Hermitian codes

Chiara Marcolla [a], Marco Pellegrini [b], Massimiliano Sala [a]

[a] Department of Mathematics, University of Trento, Italy
[b] Department of Mathematics, University of Firenze, Italy

ARTICLE INFO

Article history:
Received 28 April 2014
Accepted 19 February 2015
Available online 5 March 2015

Keywords:
Affine-variety code
Hamming weight
Hermitian code
Hermitian curve
Linear code
Minimum-weight words

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.

1. Introduction

Let q be a power of a prime, then the *Hermitian curve* $\mathcal{H}$ 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 (Ruck and Stichtenoth, 1994). This is the best known example of maximal curve and there is a vast literature on its properties, see Hirschfeld et al. (2008) for a recent survey. Moreover, the Goppa code (Goppa, 1981, 1988) constructed on this curve is by far the most studied, due to the simple basis of its Riemann–Roch space (Stichtenoth, 1993), which can be written explicitly. The Goppa construction has been generalized in

E-mail addresses: chiara.marcolla@unitn.it (C. Marcolla), pellegrin@math.unifi.it (M. Pellegrini), maxsalacodes@gmail.com (M. Sala).

http://dx.doi.org/10.1016/j.jsc.2015.03.003
0747-7171/

Vlăduţ and Manin (1984) to higher dimensions. A simpler description can be found in Fitzgerald and Lax (1998) for 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 code. In Augot (1996) the solving of a (multivariate) polynomial equation system was proposed for the first time to determine minimum-weight codewords of cyclic codes, while in Sala (2007) a more efficient system was proposed. Our proposal can be seen as a generalization to the affine-variety case of Sala (2007). A similar approach can be used to decode codes, as described, for example, in de Boer and Pellikaan (1999) and surveyed in Mora and Orsini (2009). The specialization of our results to the Hermitian case allows us to give explicit formulas for the number of some small-weight codewords. Codes over the Hermitian curve have been studied along the years and in Høholdt et al. (1998), along with a survey of known results, a new challenging approach as explicit evaluation codes is proposed. We expand on our 2006 previous result, presented orally as Sala and Pellegrini (2006), 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 code 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 Høholdt et al. (1998), and we give our algebraic characterization of fixed-weight codewords of some Hermitian codes. We study in depth the first phase (that is, $d \leq q$) in Section 3.2 and we use these results to completely classify geometrically the minimum-weight codewords for all first-phase codes in Section 3.3. In Section 3.4 we can count some special configurations of second weight codewords for any first-phase code and finally in Section 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 relies on our results (Marcolla et al., 2014) on intersection properties of $\mathcal{H}$ with some special conics, firstly 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 codes

From now on we consider $\mathbb{F}_q$ the finite field with q elements, where q is a power of a prime and $\mathbb{F}_{q^2}$ the finite field with q^2 elements. Also, $\overline{\mathbb{F}}_{q^2}$ will denote the algebraic closure of $\mathbb{F}_q$ and $\mathbb{F}_{q^2}$. Let α 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, α and β are understood as above.

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

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

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 $x \in \mathbb{F}_{q^2}$, Eq. (1) has exactly q distinct solutions in $\mathbb{F}_{q^2}$. The curve contains also one point at infinity P_∞, so it has $q^3 + 1$ rational points over $\mathbb{F}_{q^2}$ (Ruck and Stichtenoth, 1994).

Let $t \geq 1$. For any ideal I in the polynomial ring $\mathbb{F}_q[X]$, where $X = \{x_1, \ldots, x_t\}$, we denote by $\mathcal{V}(I) \subset (\overline{\mathbb{F}}_q)^t$ its variety, that is, the set of its common roots. For any $Z \subset (\overline{\mathbb{F}}_q)^t$ we denote by $\mathcal{I}(Z) \subset \mathbb{F}_q[X]$ the vanishing ideal of Z, that is, $\mathcal{I}(Z) = \{f \in \mathbb{F}_q[X] \mid f(Z) = 0\}$.

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 $\{x_1^q - x_1, \ldots, x_t^q - x_t\} \subset I$. Then I is zero-dimensional and radical (Seidenberg, 1974). Let $\mathcal{V}(I) = \{P_1, \ldots, P_n\}$.

We have an isomorphism of $\mathbb{F}_q$-vector spaces (an *evaluation map*):

$$\begin{aligned} \phi : R = \mathbb{F}_q[x_1, \ldots, x_t]/I &\longrightarrow (\mathbb{F}_q)^n \\ f &\longmapsto (f(P_1), \ldots, f(P_n)). \end{aligned} \tag{2}$$

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 from Fitzgerald and Lax (1998) and follows instead that in Marcolla et al. (2012). Let L be linearly generated by $b_1, \ldots, b_r$ then the matrix

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

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

For more recent results on affine-variety codes see Geil (2008), Marcolla et al. (2012), Lax (2012).

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 $\mathrm{w}(c)$, is the number of components of c that are different from zero and

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

Let $c \in (\mathbb{F}_q)^n$, $c = (c_1, \ldots, c_n)$. Then

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

Proposition 1. *Let $1 \leq w \leq n$. Let $I = \langle g_1, \ldots, g_s \rangle$ be such that $\{x_1^q - x_1, \ldots, x_t^q - x_t\} \subset I$. Let L be a subspace of $\mathbb{F}_{q^2}[x_1, \ldots, x_t]/I$ of dimension r. Let L be linearly generated by $\{b_1, \ldots, b_r\}$. Let J_w be the ideal in $\mathbb{F}_q[x_{1,1}, \ldots, x_{1,t}, \ldots, x_{w,1}, \ldots, x_{w,t}, z_1, \ldots, z_w]$ generated by*

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

$$g_h(x_{i,1}, \ldots, x_{i,t}) \quad \text{for} \quad i = 1, \ldots, w \text{ and } h = 1, \ldots, s \tag{5}$$

$$z_i^{q-1} - 1 \quad \text{for} \quad i = 1, \ldots, w \tag{6}$$

$$\prod_{1 \leq l \leq t} ((x_{j,l} - x_{i,l})^{q-1} - 1) \quad \text{for} \quad 1 \leq j < i \leq w. \tag{7}$$

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 σ be a permutation, $\sigma \in S_w$. It induces a permutation $\hat{\sigma}$ acting on $\{x_{1,1}, \ldots, x_{1,t}, \ldots, x_{w,1}, \ldots, x_{w,t}, z_1, \ldots, z_w\}$ 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 $Q = (\bar{x}_{1,1}, \ldots, \bar{x}_{1,t}, \ldots, \bar{x}_{w,1}, \ldots, \bar{x}_{w,t}, \bar{z}_1, \ldots, \bar{z}_w) \in \mathcal{V}(J_w)$. We can associate a codeword to Q in the following way. For each $i = 1, \ldots, w$, $P_{r_i} = (\bar{x}_{i,1}, \ldots, \bar{x}_{i,t})$ is in $\mathcal{V}(I)$, by (5). We can assume

$r_1 < r_2 < \ldots < r_w$, 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 an l such that $x_{i,l} \neq x_{j,l}$. Since $\bar{z}_i^{q-1} = 1$ (6), $\bar{z}_i \in \mathbb{F}_q \setminus \{0\}$. Let $c \in (\mathbb{F}_q)^n$ be

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

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 $w!$. □

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. The **norm** $\mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}}$ and the **trace** $\mathrm{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}}$ are two functions from $\mathbb{F}_{q^m}$ to $\mathbb{F}_q$ such that

$$\mathrm{N}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}}(x) = x^{1+q+\ldots+q^{m-1}} \quad \text{and} \quad \mathrm{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^m}}(x) = x + x^q + \ldots + x^{q^{m-1}}.$$

We denote by N and Tr, respectively, the norm and the trace from $\mathbb{F}_{q^2}$ to $\mathbb{F}_q$. It is clear that $\mathcal{H} = \{\mathrm{N}(x) = \mathrm{Tr}(y) \mid x, y \in \overline{\mathbb{F}}_{q^2}\}$.

Lemma 1. *For any $t \in \mathbb{F}_q$, the equation $\mathrm{Tr}(y) = y^q + y = t$ has exactly q distinct solutions in $\mathbb{F}_{q^2}$. The equation $\mathrm{N}(x) = x^{q+1} = t$ 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 $\mathbb{F}_q$-vector spaces of dimension, respectively, 2 and 1. Thus, $\dim(\ker(\mathrm{Tr})) = 1$, and this means that for any $t \in \mathbb{F}_q$ the set of solutions of the equation $\mathrm{Tr}(y) = y^q + y = t$ is non-empty and then it has the same cardinality of $\mathbb{F}_q$, that is, q.*

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

Lemma 2. *Let $\mathcal{H}$ be the Hermitian curve.*

(i) *Every line $\mathcal{L}$ of $\mathbb{P}^2(\mathbb{F}_{q^2})$ either intersects $\mathcal{H}$ in $q + 1$ distinct points, or it is tangent to $\mathcal{H}$ at a point P (with contact order $q + 1$). In the latter case, $\mathcal{L}$ does not intersect $\mathcal{H}$ in any other point different from P.*
(ii) *Through each point of $\mathcal{H}$, there is one tangent and q^2 lines of $\mathbb{P}^2(\mathbb{F}_{q^2})$ that intersect $\mathcal{H}$ in $q + 1$ points.*

Proof. See Hirschfeld (1998), Lemma 7.3.2 at p. 247. □

Lemma 3. *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 $t \in \mathbb{F}_{q^2}$, $t^{q+1} \in \mathbb{F}_q$, and so the equation $y^q + y = t^{q+1}$ has exactly q distinct solutions by applying Lemma 1. □

Lemma 4. *Let $\mathcal{L}$ be any horizontal line $\{y = b\}$, with $b \in \mathbb{F}_{q^2}$. Then if $\mathrm{Tr}(b) = 0$, $\mathcal{L}$ intersects $\mathcal{H}$ in one affine point, otherwise, if $\mathrm{Tr}(b) \neq 0$, $\mathcal{L}$ intersects $\mathcal{H}$ in $q + 1$ affine points.*

Proof. By Lemma 1, for any $b \in \mathbb{F}_{q^2}$, the equation $x^{q+1} = b^q + b$ has exactly $q + 1$ distinct solutions if $\mathrm{Tr}(b) \neq 0$, otherwise it has one solution. □

Lemma 5. *In the affine plane $\mathbb{A}^2(\mathbb{F}_{q^2})$, the total number of non-vertical lines is q^4. Of these, $q^4 - q^3$ intersect $\mathcal{H}$ in $q+1$ affine points, while the remaining q^3 lines are tangent to $\mathcal{H}$ and they intersect $\mathcal{H}$ in only one affine point.*

Proof. Let $\mathcal{L}$ be any non-vertical line in $\mathbb{A}^2(\mathbb{F}_{q^2})$, then $\mathcal{L} = \{y = ax + b\}$, with $a, b \in \mathbb{F}_{q^2}$. We have q^2 choices for both a and b, so the total number is q^4.

By (ii) of Lemma 2 we have that through each point of $\mathcal{H}$ there is one tangent. Since the Hermitian curve has q^3 affine points, then there exist q^3 tangent lines to $\mathcal{H}$ (that meet $\mathcal{H}$ at a single point of order $q+1$).

The lines containing the point at infinity are only the vertical lines. By Lemma 3, their number is q^2 (since they are $\mathcal{L} = \{x = t\}$ where $t \in \mathbb{F}_{q^2}$).

The remaining lines are $q^4 - q^3$. By (i) of Lemma 2 they meet the curve at $q+1$ affine points. □

3. Small-weight codewords of Hermitian codes

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

Let $I = \langle x^{q+1} - y^q - y, x^{q^2} - x, y^{q^2} - y \rangle \subset \mathbb{F}_{q^2}[x, y]$ 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 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 have the following affine-variety codes: $C(I, L) = \mathrm{Span}_{\mathbb{F}_{q^2}} \langle \phi(\mathcal{B}_{m,q}) \rangle$ where ϕ is the evaluation map (2) 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:

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

Remark 1. We recall that the *Riemann–Roch space* associated to a divisor E of a curve χ is a vector space $\mathcal{L}(E)$ over $\mathbb{F}_q(\chi)$ defined as

$$\mathcal{L}(E) = \{f \in \mathbb{F}_q(\chi) \mid (f) + E \geq 0\} \cup \{0\},$$

where $\mathbb{F}_q(\chi)$ is a *rational function field* on χ. In particular, if we consider the Hermitian curve $\mathcal{H}$, we know that it has $q^3 + 1$ points of degree one, namely a pole Q_∞ and q^3 distinct affine points $P_{\gamma,\delta} = (\gamma, \delta)$ such that $\gamma^{q+1} = \delta^q + \delta$. Let D be the divisor $D = \sum_{\gamma^{q+1} = \delta^q + \delta} P_{\gamma,\delta}$ on the curve $\mathcal{H}$. For $m \in \mathbb{Z}$ the affine-variety code $C(m, q)^\perp$ is the same code as the Goppa code $C(D, mQ_\infty)$ associated with the divisors D and mQ_∞ as

$$C(D, mQ_\infty) = \{(f(P_1), \dots, f(P_n)) \mid f \in \mathcal{L}(mQ_\infty)\} \subset (\mathbb{F}_{q^2})^n,$$

where $\mathcal{L}(mQ_\infty)$ is a vector space over $\mathbb{F}_{q^2}(\mathcal{H})$.

Note that $\mathcal{B}_{m,q}$ is a monomial basis for $\mathcal{L}(mQ_\infty)$.

The Hermitian codes can be divided in four phases (Høholdt et al., 1998), any of them having specific explicit formulas linking their dimension and their distance (Marcolla, 2013), as in Table 1.

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

Table 1
The four "phases" of Hermitian codes (Marcolla, 2013).

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

3.1. Corner codes and edge codes

In Section 5.3 of Høholdt et al. (1998), the first phase denotes case (3) at p. 933, where it is characterized by $l < g$, which is equivalent to consider the first $g-1$ nongaps in the numerical semigroup $\Lambda = \langle q, q+1 \rangle$, that is all nongaps up to the conductor $c = 2g = q^2-q$. With respect to this description, we are able to extend this phase to include also nongaps $\{q^2-q+1, \ldots, q^2-2\}$, as follows.

By analyzing precisely the monomials involved, we are able to partition this phase in two sets: the *edge codes* and the *corner codes*. When considering nongaps up to the conductor, there are nongaps immediately preceding a gap. These correspond to *corner codes*. The others are *edge codes*. For example, if $\Lambda = \langle 5, 6 \rangle$ then $g = 10$ and the conductor $c = 20$. The non-gaps up to c are $\{0, 5, 6, 10, 11, 12, 15, 16, 17, 18, 20\}$. Obviously, $\{0, 6, 12, 18\}$ are followed by the gaps, respectively, $\{1, 7, 13, 19\}$. So $\{0, 6, 12, 18\}$ correspond to corner codes, while $\{5, 10, 11, 15, 16, 17, 20, 21, 22, 23\}$ correspond to edge codes (note that we have included our addition $\{21, 22, 23\}$, with $q^2-2 = 23$).

We observe that corner codes are codes of the form $C(m, q)$, with $m = (q+1)s$ and $0 \le s \le q-2$, while edge codes are codes of the form $C(m, q)$, with $m = qr+(q+1)s$, $1 \le r \le q-1$ and $r+s \le q-1$.

We provide a formal definition in terms of monomials.

Definition 3. Let $2 \le d \le q$ and let $1 \le j \le d-1$.
Let $L_d^0 = \{1, x, \ldots, x^{d-2}\}, L_d^1 = \{y, xy, \ldots, x^{d-3}y\}, \ldots, L_d^{d-2} = \{y^{d-2}\}$.
Let $l_d^1 = x^{d-1}, \ldots, l_d^j = x^{d-j}y^{j-1}$.

- If $\mathcal{B}_{m,q} = L_d^0 \cup \ldots \cup L_d^{d-2}$, then we say that $C(m, q)$ is a **corner code** and we denote it by H_d^0.
- If $\mathcal{B}_{m,q} = L_d^0 \cup \ldots \cup L_d^{d-2} \cup \{l_d^1, \ldots, l_d^j\}$, then we say that $C(m, q)$ is an **edge code** and we denote it by H_d^j.

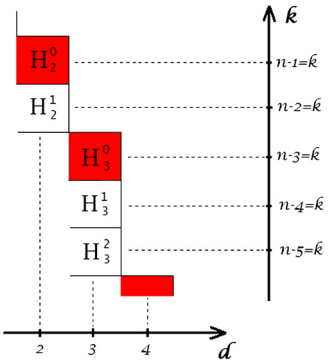
From the formulas in Table 1 we have the following theorem.

Theorem 4. *Let $2 \le d \le q$, $1 \le j \le d-1$. Then*

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

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 an $[n, n-1, 2]$ code.
$\mathcal{B}_{m,q} = L_2^0 = \{1\}$, so the parity-check matrix of H_2^0 is $(1, \ldots, 1)$.
H_2^1 is an $[n, n-2, 2]$ code.
$\mathcal{B}_{m,q} = L_2^0 \cup \{l_2^1\} = \{1, x\}$
H_3^0 is an $[n, n-3, 3]$ code.
$\mathcal{B}_{m,q} = L_3^0 \cup L_3^1 = \{1, x, y\}$
H_3^1 is an $[n, n-4, 3]$ code.
$\mathcal{B}_{m,q} = L_3^0 \cup L_3^1 \cup \{l_3^1\} = \{1, x, y, x^2\}$
H_3^2 is an $[n, n-5, 3]$ code.
$\mathcal{B}_{m,q} = L_3^0 \cup L_3^1 \cup \{l_3^1, l_3^2\} = \{1, x, y, x^2, xy\}$



3.2. First results for the first phase

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

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

Let $w \ge v \ge 1$. Let $Q = (\bar{x}_1, \ldots, \bar{x}_w, \bar{y}_1, \ldots, \bar{y}_w, \bar{z}_1, \ldots, \bar{z}_w) \in \mathcal{V}(J_w)$. We know (see Proposition 1) that Q correspond to a codeword c. We say that the set $\{(\bar{x}_1, \bar{y}_1), \ldots, (\bar{x}_w, \bar{y}_w)\}$ is the **support** of c.

We say that Q is in v**-block position** if we can partition $\{1, \ldots, w\}$ in v blocks $I_1, \ldots, I_v$ such that

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

This means that, in the support of c, we have $|I_1|$ points on a vertical line, $|I_2|$ points on another vertical line, and so on.

W.l.o.g. we can assume $|I_1| \le \ldots \le |I_v|$ and $I_1 = \{1, \ldots, u\}$.

We need the following technical lemmas.

Lemma 6. *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 $u + v \le \lfloor \frac{w}{2} \rfloor + 2$.*

Proof. Note that $uv \le w$ since $|I_1| + \ldots + |I_v| = w$ and $|I_1| \le \ldots \le |I_v|$. So the worst case is when $w = uv$. This is equivalent to the case when all blocks have the same size. Let $w' := uv$, note that we always have $w' \le w$ and hence any lower bound for w' implies a lower bound for w. If $u = 1$, then we have $u + v = 1 + v = 1 + w'$. If $v = 1$, then $u = w = w'$ and so $u + v = w + 1$. If $u \ge 2$ and $v \ge 2$, we have $u \le \lfloor \frac{w}{2} \rfloor$ and $v \le \lfloor \frac{w}{2} \rfloor$, and then $u + v \le \lfloor \frac{w}{2} \rfloor + \lfloor \frac{w}{2} \rfloor \le w < w + 1$. So we always have $u + v \le w + 1$.

To prove that $u + v \le \lfloor \frac{w}{2} \rfloor + 2$, we study the real-valued function $f(v) = u + v = \frac{w}{v} + v$, with $2 \le v \le \frac{w}{2}$ ($w \ge 4$). We have $f(2) = f(\frac{w}{2}) = \frac{w}{2} + 2$ where $v = \sqrt{w}$ is the minimum point. In fact, the derivative of f (in the variable v) is $f'(v) = (v^2 - w)/v^2$, its zero is $v = \sqrt{w}$, f'' is positive in the whole interval under consideration and we have $2 \le \sqrt{w} \le \frac{w}{2}$. Thus, the function takes its maximum value at the endpoints of the interval. Then we have $u + v \le \frac{w}{2} + 2$. Since u and v are integers, we actually have that $u + v \le \lfloor \frac{w}{2} \rfloor + 2$. □

Lemma 7. *Let us consider the edge code H_d^j with $1 \le j \le d - 1 \le q - 1$ and $3 \le d \le w \le 2d - 3$. Let $Q = (\bar{x}_1, \ldots, \bar{x}_w, \bar{y}_1, \ldots, \bar{y}_w, \bar{z}_1, \ldots, \bar{z}_w)$ be a solution of J_w in v-block position, then exactly one of the following cases holds:*

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

or

(b) $v = 1$, *that is,* $\bar{x}_1 = \ldots = \bar{x}_w$.

Proof. We define, for all h such that $1 \leq h \leq v$:

$$X_h = \bar{x}_i \quad \text{if } i \in I_h, \qquad Z_h = \sum_{i \in I_h} \bar{z}_i.$$

(a) $u = 1$. We want to prove, by contradiction, that $v \geq d+1$.
Let $v \leq d$. Since $Q \in \mathcal{V}(J_w)$, for any $f \in L_d^0, \{l_d^1\}$ we have $f(Q) = 0$ and so we have the following equations

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

Since $v \leq d$, one can restrict to the first v equations of (10) to get a $v \times v$ system, that is,

$$\begin{pmatrix} 1 & \ldots & 1 \\ X_1 & \ldots & X_v \\ \vdots & \ddots & \vdots \\ X_1^{v-1} & \ldots & X_v^{v-1} \end{pmatrix} \begin{pmatrix} Z_1 \\ \vdots \\ Z_v \end{pmatrix} = 0 \tag{11}$$

The above matrix is a Vandermonde matrix and the X_i's are pairwise distinct, so it has maximal rank v. Therefore, the solution of (11) is $(Z_1, \ldots, Z_v) = (0, \ldots, 0)$. Since $u = 1$, then $Z_1 = \bar{z}_1 = 0$, which contradicts $\bar{z}_i \in \mathbb{F}_{q^2} \setminus \{0\}$. Thus, $v \geq d+1$; we have $w+1 \geq u+v = v+1 > d+1$ and hence $w \geq d+1$.

(b) $u \geq 2$. We suppose by contradiction that $v \geq 2$.
We need to define:

$$Y_{h,s} = \sum_{i \in I_h} \bar{y}_i^s \bar{z}_i \quad \text{with } 1 \leq s \leq u-1$$

We consider Proposition 1. A subset of equations of condition (4) is the following system:

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

In fact, system (12) is a subset of (4) if and only if $\deg(\bar{x}_i^{v-1} \bar{y}_i^{u-1}) \leq d-2$ for any $i = 1, \ldots, w$. That is, $(v-1) + (u-1) \leq d-2 \iff v+u \leq d$.
To verify this, since $v \geq 2$, it is sufficient to apply Lemma 6 and we obtain $u + v \leq \lfloor \frac{w}{2} \rfloor + 2 \leq \lfloor \frac{2d-3}{2} \rfloor + 2 = d$.
System (12) can be decomposed in u systems, all with the same Vandermonde matrix, having rank v:

$$\begin{cases} \sum_{h=1}^{v} Z_h = 0 \\ \sum_{h=1}^{v} X_h Z_h = 0 \\ \quad \vdots \\ \sum_{h=1}^{v} X_h^{v-1} Z_h = 0 \end{cases}, \begin{cases} \sum_{h=1}^{v} Y_{h,1} = 0 \\ \sum_{h=1}^{v} X_h Y_{h,1} = 0 \\ \quad \vdots \\ \sum_{h=1}^{v} X_h^{v-1} Y_{h,1} = 0 \end{cases}, \ldots, \begin{cases} \sum_{h=1}^{v} Y_{h,u-1} = 0 \\ \sum_{h=1}^{v} X_h Y_{h,u-1} = 0 \\ \quad \vdots \\ \sum_{h=1}^{v} X_h^{v-1} Y_{h,u-1} = 0 \end{cases} \tag{13}$$

Therefore, the solutions of these systems are zero-solutions. So, in particular, we have $Z_1 = Y_{1,1} = \ldots = Y_{1,u-1} = 0$, that is

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

Since the $\bar{x}_i$'s in I_1 are all equal, then the $\bar{y}_i$'s are all distinct. Then the last Vandermonde matrix has rank u, and so $\bar{z}_1 = \ldots = \bar{z}_u = 0$, but this is impossible because every $\bar{z}_i \in \mathbb{F}_{q^2} \setminus \{0\}$. Therefore $v = 1$ and $u = w$. □

3.3. Minimum-weight codewords

Corollary 1. *Let us consider the edge code H_d^j with $1 \le j \le d-1 \le q-1$.*

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 $\bar{x}_1 = \ldots = \bar{x}_d$. In other words, the support of a minimum-weight word lies in the intersection of the Hermitian curve $\mathcal{H}$ and a vertical line.

Whereas if $d \ge 4$ 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) $\bar{x}_i \ne \bar{x}_j$ *for* $i \ne j$, $1 \le i, j \le d+1$,

or

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

Proof. We are in the hypotheses of Lemma 7. If $w = d$, then $u > 1$, hence $v = 1$. Whereas, if $w = d+1$, we can apply Lemma 7 only if $d \ge 4$. We have two possibilities: in case (a) of Lemma 7, we have $v = d+1$, then all $\bar{x}_i$'s are different, otherwise we are in case (b). □

Now we can prove the following theorem for edge codes.

Theorem 5. *Let $2 \le d \le q$ and let $1 \le j \le d-1$, then 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 the words of minimum weight. The first set of ideal basis (9) has exactly $\frac{d(d-1)}{2} + j$ equations, where $1 \le j \le d-1$. So, if $j = 1$, this set implies the following system:

$$\begin{cases} \bar{z}_1 + \ldots + \bar{z}_d = 0 \\ \bar{x}_1\bar{z}_1 + \ldots + \bar{x}_d\bar{z}_d = 0 \\ \bar{y}_1\bar{z}_1 + \ldots + \bar{y}_d\bar{z}_d = 0 \\ \quad \vdots \\ \bar{y}_1^{d-2}\bar{z}_1 + \ldots + \bar{y}_d^{d-2}\bar{z}_d = 0 \\ \bar{x}_1^{d-1}\bar{z}_1 + \ldots + \bar{x}_d^{d-1}\bar{z}_d = 0 \end{cases} \tag{14}$$

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

$$\begin{cases} \bar{x}_1^{d-2}\bar{y}_1\bar{z}_1 + \ldots + \bar{x}_d^{d-2}\bar{y}_d\bar{z}_d = 0 \\ \bar{x}_1^{d-3}\bar{y}_1^2\bar{z}_1 + \ldots + \bar{x}_d^{d-3}\bar{y}_d^2\bar{z}_d = 0 \\ \quad\vdots \\ \bar{x}_1\bar{y}_1^{d-2}\bar{z}_1 + \ldots + \bar{x}_d\bar{y}_d^{d-2}\bar{z}_d = 0 \end{cases} \tag{15}$$

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

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

We have q^2 choices for the common value of the $\bar{x}_i$'s and, by Lemma 3, we have $\binom{q}{d}d!$ different $\bar{y}_i$'s, since for any choice of $\bar{x}_i$ 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.

The matrix of the system (16) is a Vandermonde matrix, with rank $d-1$. This means that the solution space has linear dimension 1. 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 the $\bar{y}_i$'s. So the number of the $\bar{z}_i$'s is $|\mathbb{F}_{q^2}^*| = q^2 - 1$, then $A_d = \frac{1}{d!}\left(q^2\binom{q}{d}d!(q^2-1)\right)$. □

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

Proposition 2. *Let us consider the corner code H_d^0 and $2 \le d \le q$. Then the points $(\bar{x}_1, \bar{y}_1), \ldots, (\bar{x}_d, \bar{y}_d)$ corresponding to minimum-weight words lie on a 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,

$$\begin{cases} \bar{z}_1 + \ldots + \bar{z}_d = 0 \\ \bar{x}_1\bar{z}_1 + \ldots + \bar{x}_d\bar{z}_d = 0 \\ \bar{y}_1\bar{z}_1 + \ldots + \bar{y}_d\bar{z}_d = 0 \\ \quad\vdots \\ \bar{y}_1^{d-2}\bar{z}_1 + \ldots + \bar{y}_d^{d-2}\bar{z}_d = 0 \end{cases} \tag{17}$$

This system is the same as (14), but with a missing equation. This means that (17) has all the solutions of system (14) and other solutions.

We claim that the $\bar{z}_i$'s are all non-zero only if either all $\bar{x}_i$'s are distinct, or all are equal. In fact, suppose that we have some (but not all) $\bar{x}_i$'s equal, then we have that the point $Q \in \mathcal{V}(J_w)$, that corresponds to a codeword c, is in v-block position with $1 < v < d$. We can repeat the same argument of the proof of Lemma 7. In particular, we have two different cases:

- $u = 1$ we can restrict to the first v of equations of a subset of (17), which has just the variables x's and z's. In this way we obtain a $v \times v$ system as (11). As before, $\bar{z}_1 = 0$ since $u = 1$, so it is impossible.
- $u \ge 2$ and $v \ge 2$. We have u systems, all with the same Vandermonde matrix, having rank v as (13). As in the point (b) of the proof of Lemma 7, we obtain that $\bar{z}_1 = \ldots = \bar{z}_u = 0$.

Therefore, we have only two possibilities for the $\bar{x}_i$'s: either all are different or they coincide. The same consideration is true for the $\bar{y}_i$'s, because when we consider (17) and we exchange x with y, we obtain again (17).

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. Substituting the above transformation in (17) and applying some operations between the equations, we obtain a system that is equivalent to (17). 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 a same line. □

We finally prove the following theorem:

Theorem 6. *Let $2 \leq d \leq q$, then the number of words having weight d of a corner code H_d^0 is*

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

Proof. Again, the points corresponding to minimum-weight words of a corner code have to verify (17). By Proposition 2, we know that these points lie in the intersections of any line and the Hermitian curve $\mathcal{H}$.

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

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

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 5 we have that the number of d-tuples of points is

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

because we have q^4-q^3 non-vertical lines that intersect $\mathcal{H}$ in $q+1$ points, and for any choice of a line we need just d of these points (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 (17).

We apply an affine transformation to the system (17) 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 (16). Therefore we have a Vandermonde matrix, hence the number of the $\bar{z}_i$'s is q^2-1. So

$$\begin{aligned} A_d &= \tfrac{1}{d!}\left(q^2(q^2-1)\tbinom{q}{d}d! + (q^4-q^3)(q^2-1)\tbinom{q+1}{d}d!\right) \\ &= q^2(q^2-1)\left[\tbinom{q}{d} + (q^2-q)\tbinom{q+1}{d}\right] = \\ &= q^2(q^2-1)\left[\tfrac{(q-d+1)q!}{d(d-1)!(q-d+1)!} + (q^2-q)\tfrac{(q+1)q!}{d(d-1)!(q-d+1)!}\right] \\ &= q^2(q^2-1)\tbinom{q}{d-1}\left[\tfrac{q-d+1}{d} + \tfrac{(q^2-q)(q+1)}{d}\right] = q^2(q^2-1)\tfrac{q^3-d+1}{d}\tbinom{q}{d-1}. \qquad \square \end{aligned}$$

3.4. Second-weight codewords

In this section we state more theorems for edge and corner codes. We study the case when the $\bar{x}_i$'s coincide or when the $\bar{y}_i$'s coincide.

Theorem 7. *Let $2 \leq d \leq q$, then the number of words of weight $d+1$ with $\bar{y}_1 = \ldots = \bar{y}_{d+1}$ of a corner code H^0_d is:*

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

Whereas for an edge code H^j_d with $1 \leq j \leq d-1$ this numbers is:

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

Proof. We have q^2-q choices for the $\bar{y}_i$'s and, by Lemma 4, we have $\binom{q+1}{d+1}(d+1)!$ different $\bar{x}_i$'s, 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 $d+1$ 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, in the two distinct cases.

- **Case** H^0_d. By Proposition 1 we know that J_d represents all the words of minimum weight. The first set of ideal basis (9) has exactly $\frac{d(d-1)}{2}$ equations, which is system (17) with more variables.[1] Since $\bar{y}_1 = \ldots = \bar{y}_{d+1}$, system (17) becomes

$$\begin{cases} \bar{z}_1 + \ldots + \bar{z}_{d+1} = 0 \\ \bar{x}_1\bar{z}_1 + \ldots + \bar{x}_{d+1}\bar{z}_{d+1} = 0 \\ \quad\vdots \\ \bar{x}_1^{d-2}\bar{z}_1 + \ldots + \bar{x}_{d+1}^{d-2}\bar{z}_{d+1} = 0 \end{cases} \tag{18}$$

  The matrix of this system is a Vandermonde matrix of rank $d-1$. This means that the solution space has linear dimension 2, hence the number of the admissible z's is $q^4 - |\{\bar{z}_i = 0 \text{ for at least one } i\}|$. Now we compute the number of solutions such that $\bar{z}_i = 0$ for at least one i. If we set one $\bar{z}_i = 0$, we have a linear (solution) space of dimension 1, that contains q^2 solutions, corresponding to the zero solution and q^2-1 codewords of weight d. We have $d+1$ of such subspaces.
  Moreover, the intersection of any two of them is only the zero solution, because if we set $\bar{z}_i = 0$ for two $\bar{z}_i$'s, we have a linear space of dimension 0. The number of admissible z's is $q^4-(d+1)q^2+d$, obtained by counting the elements of $d+1$ subspaces and removing the zero solution counted d extra times. Thus, the number of words of weight $d+1$ with $\bar{y}_1 = \ldots = \bar{y}_{d+1}$ of H^0_d is:

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

- **Case** H^j_d. In this case the first set of ideal basis (9) contains exactly $\frac{d(d-1)}{2}+j$ equations, where $1 \leq j \leq d-1$. So, if $j=1$, this set implies the system (14) with more variables. Whereas, if $j>1$, then we have to add the first $j-1$ of Eqs. (15) with more variables.

[1] We have $\bar{x}_i$, $\bar{y}_i$, $\bar{z}_i$ with $1 \leq i \leq d+1$ instead of $1 \leq i \leq d$. We mean this every time that we write "with more variables".

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

$$\begin{cases} \bar{z}_1 + \ldots + \bar{z}_{d+1} = 0 \\ \bar{x}_1\bar{z}_1 + \ldots + \bar{x}_{d+1}\bar{z}_{d+1} = 0 \\ \quad \vdots \\ \bar{x}_1^{d-1}\bar{z}_1 + \ldots + \bar{x}_{d+1}^{d-1}\bar{z}_{d+1} = 0 \end{cases} \tag{19}$$

This means that the solution space has linear dimension 1. So the number of the z's is $|\mathbb{F}_{q^2}^*| = q^2 - 1$, then the number of words of weight $d+1$ with $\bar{y}_1 = \ldots = \bar{y}_{d+1}$ of H_d^j is

$$(q^2 - q)(q^2 - 1)\binom{q+1}{d+1}. \qquad \square$$

Theorem 8. *Let $2 \le d \le q-1$, then the number of words of weight $d+1$ with $\bar{x}_1 = \ldots = \bar{x}_{d+1}$ 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 1 we know that J_d represents all the words of minimum weight. For an edge code the first set of ideal basis (9) implies, if $j = 1$, the system (14) with more variables and, if $j > 1$, we have to add the first $j-1$ of Eqs. (15) with more variables. Whereas, for a corner code, the first set of ideal basis (9) implies the system (17) with more variables.

But $\bar{x}_1 = \ldots = \bar{x}_{d+1}$, so in both cases the system becomes:

$$\begin{cases} \bar{z}_1 + \ldots + \bar{z}_{d+1} = 0 \\ \bar{y}_1\bar{z}_1 + \ldots + \bar{y}_{d+1}\bar{z}_{d+1} = 0 \\ \quad \vdots \\ \bar{y}_1^{d-2}\bar{z}_1 + \ldots + \bar{y}_{d+1}^{d-2}\bar{z}_{d+1} = 0 \end{cases} \tag{20}$$

We have q^2 choices for the $\bar{x}_i$'s and, by Lemma 3, 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. Moreover, we have $(q^4 - (d+1)q^2 + d)$ possible z's, because system (20) is analogous to the system (18). $\square$

Theorem 9. *Let $2 \le d \le q$, then the number of words of weight $d+1$ of a corner code H_d^0 with $(\bar{x}_i, \bar{y}_i)$ lying on a non-vertical line is:*

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

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

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

Proof (sketched). We have $q^4 - q^3$ non-vertical lines, intersecting $\mathcal{H}$ in a set of $q+1$ points. We choose a line and $d+1$ points on it. By an affine transformation, the system can always be reduced to system (18) for corner codes, or to system (19) for edge codes. For corner codes we get a linear space of dimension 2, whereas for edge codes we get a linear space of dimension 1. $\square$

Remark 2. Non-vertical lines include horizontal lines of Theorem 7, so that Theorem 9 can be considered as a generalization of Theorem 7.

In other cases, we have to consider the intersection of $\mathcal{H}$ with higher degree curves and the formulas get more complicated. For example, the cubic found in Couvreur (2012).

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

In this section we will study separately some special cases of Hermitian codes, that is, the corner codes and edge codes of distance $d = 3$ and $d = 4$, with $q \geq 3$: H_3^0, H_3^1, H_3^2, H_4^0, $\{\mathsf{H}_4^j\}_{1 \leq j \leq 3}$. For any of these codes, we count the number of words having weight $d + 1$. In the following section we are going to prove these theorems:

Theorem 10. *Let $q \geq 3$. The number of words of weight 4 of a corner code H_3^0 is:*

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

The number of words of weight 4 of an edge code H_3^1 is[2]*:*

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

where N_k is the number of parabolas (of the form $y = ax^2 + bx + c$, $a \neq 0$ and $a, b, c \in \mathbb{F}_{q^2}$) and non-vertical lines that intersect $\mathcal{H}$ in exactly k points.

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

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

Theorem 11. *Let $q \geq 4$. The number of words of weight 5 of a corner code H_4^0 is:*

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

The number of words of weight 5 of all edge codes H_4^j for $1 \leq j \leq 3$ is:

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

The formula for A_4 of H_3^1 in Theorem 10 contains some implicit values N_k's. To derive explicit values it is enough to consider Theorem 3.1 of Marcolla et al. (2014).

3.5.1. Study of H_3^0

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

$$\begin{cases} \bar{z}_1 + \bar{z}_2 + \bar{z}_3 + \bar{z}_4 = 0 \\ \bar{x}_1\bar{z}_1 + \bar{x}_2\bar{z}_2 + \bar{x}_3\bar{z}_3 + \bar{x}_4\bar{z}_4 = 0 \\ \bar{y}_1\bar{z}_1 + \bar{y}_2\bar{z}_2 + \bar{y}_3\bar{z}_3 + \bar{y}_4\bar{z}_4 = 0 \end{cases}$$

This is a linear system in $\bar{z}_i$. We first choose 4 distinct points $P_i = (\bar{x}_i, \bar{y}_i)$ on $\mathcal{H}$ and then we compute the number of solutions in $\bar{z}_i$'s. The coefficient matrix is

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ \bar{x}_1 & \bar{x}_2 & \bar{x}_3 & \bar{x}_4 \\ \bar{y}_1 & \bar{y}_2 & \bar{y}_3 & \bar{y}_4 \end{pmatrix}$$

[2] Note that if $q = 3$, then $\binom{q}{4} = 0$ by convention.

This matrix cannot have rank 1, since either the $\bar{x}_i$'s or the $\bar{y}_i$'s are not all equal. If the rank is 2, this means that all P_i's lie on a same line. In this case, the linear space of solutions has dimension 2, so that we have $q^4 - 4q^2 + 3$ solutions in $\bar{z}_i$'s.

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 $\bar{z}_4 = 0$, which is not admissible. Thus, if we choose 4 points such that no 3 of them lie on a same line, all $\bar{z}_i$'s will be non-zero and we get a codeword of weight 4. The vector space of solutions has dimension 1, so that we have $q^2 - 1$ solutions in $\bar{z}_i$'s.

If the rank is 2, by Lemmas 3 and 5 the total number of solutions (in $\bar{x}_i, \bar{y}_i, \bar{z}_i$) is

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

If the rank is 3, the total number of solutions (in $\bar{x}_i, \bar{y}_i, \bar{z}_i$) is

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

(We consider all the choices of 4 points of $\mathcal{H}$, then we subtract all the choices of 3 points on a line and the other elsewhere, and we also subtract all the choices of 4 points on a line.) Putting together, we get the total number of codewords of weight 4 of H_3^0:

$$A_4 = \left(\binom{q^3}{4} - q^2\binom{q}{3}(q^3 - q) - (q^4 - q^3)\binom{q+1}{3}(q^3 - q - 1)\right)(q^2 - 1) + \left(q^2\binom{q}{4} + (q^4 - q^3)\binom{q+1}{4}\right)(q^4 - 5q^2 + 4).$$

Doing the computations we obtain the first part of Theorem 10.

3.5.2. Study of H_3^1

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

$$\begin{cases} \bar{z}_1 + \bar{z}_2 + \bar{z}_3 + \bar{z}_4 = 0 \\ \bar{x}_1\bar{z}_1 + \bar{x}_2\bar{z}_2 + \bar{x}_3\bar{z}_3 + \bar{x}_4\bar{z}_4 = 0 \\ \bar{y}_1\bar{z}_1 + \bar{y}_2\bar{z}_2 + \bar{y}_3\bar{z}_3 + \bar{y}_4\bar{z}_4 = 0 \\ \bar{x}_1^2\bar{z}_1 + \bar{x}_2^2\bar{z}_2 + \bar{x}_3^2\bar{z}_3 + \bar{x}_4^2\bar{z}_4 = 0 \end{cases}$$

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

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ \bar{x}_1 & \bar{x}_2 & \bar{x}_3 & \bar{x}_4 \\ \bar{y}_1 & \bar{y}_2 & \bar{y}_3 & \bar{y}_4 \\ \bar{x}_1^2 & \bar{x}_2^2 & \bar{x}_3^2 & \bar{x}_4^2 \end{pmatrix} \tag{21}$$

Now we study the rank of the matrix according to "v-blocks" (although we cannot apply Lemma 7).

If all $\bar{x}_i$'s are equal, we have 4 points on a vertical line; the rank is 2 and the number of codewords is (see case H_3^0)

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

If only three $\bar{x}_i$'s are equal, we have 3 points on a vertical line and another one outside, but this configuration is impossible for H_3^0 (that is, we do not have codewords associated to it), and it is also impossible for H_3^1, since $\mathsf{H}_3^1 \subseteq \mathsf{H}_3^0$.

If we have two pairs of equal $\bar{x}_i$'s (for instance, $\bar{x}_1 = \bar{x}_2 \neq \bar{x}_3 = \bar{x}_4$), we can have codewords. In this case, we deduce $\bar{z}_1 + \bar{z}_2 = 0$, $\bar{z}_3 + \bar{z}_4 = 0$, $\bar{z}_1(\bar{y}_1 - \bar{y}_2) + \bar{z}_3(\bar{y}_3 - \bar{y}_4) = 0$, so that we have $\binom{q^2}{2}$ ways to choose $\{\bar{x}_1, \bar{x}_3\}$, $\binom{q}{2}$ ways to choose $\{\bar{y}_1, \bar{y}_2\}$, $\binom{q}{2}$ ways to choose $\{\bar{y}_3, \bar{y}_4\}$, $q^2 - 1$ ways to choose $\bar{z}_1$, this determines all $\bar{z}_i$. The number of codewords in this case is

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

If only two $\bar{x}_i$'s are equal, say $\bar{x}_1 = \bar{x}_2$, we can show that we have $\bar{z}_1 + \bar{z}_2 = 0$, $\bar{z}_3 = 0$, $\bar{z}_4 = 0$ (because if we set $Z_1 = \bar{z}_1 + \bar{z}_2$, we get a Vandermonde matrix of rank 3), which is not admissible.

If we have all $\bar{x}_i$'s distinct, the submatrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ \bar{x}_1 & \bar{x}_2 & \bar{x}_3 & \bar{x}_4 \\ \bar{x}_1^2 & \bar{x}_2^2 & \bar{x}_3^2 & \bar{x}_4^2 \end{pmatrix}$$

has rank 3, but if the whole matrix (21) had rank 4 we could only have the zero solution, which is not admissible. Thus, (21) must have rank 3, that is, the $\bar{y}_i$'s row must be linearly dependent on the other rows. This means that

$$\exists a, b, c \in \mathbb{F}_{q^2} \text{ such that } \bar{y}_i = a\bar{x}_i^2 + b\bar{x}_i + c \quad \forall i = 1, \ldots, 4.$$

That is, all P_i's lie on a same parabola (or on a same non-vertical line, if $a = 0$). 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 (of the form $y = ax^2 + bx + c$, $a \neq 0$ and $a, b, c \in \mathbb{F}_{q^2}$) and non-vertical lines that intersect $\mathcal{H}$ in exactly k points (any parabola can intersect $\mathcal{H}$ at most in $2q$ points).

Putting all together we get A_4, that is, the second part of Theorem 10.

3.5.3. Study of H_3^2

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

$$\begin{cases} \bar{z}_1 + \bar{z}_2 + \bar{z}_3 + \bar{z}_4 = 0 \\ \bar{x}_1\bar{z}_1 + \bar{x}_2\bar{z}_2 + \bar{x}_3\bar{z}_3 + \bar{x}_4\bar{z}_4 = 0 \\ \bar{y}_1\bar{z}_1 + \bar{y}_2\bar{z}_2 + \bar{y}_3\bar{z}_3 + \bar{y}_4\bar{z}_4 = 0 \\ \bar{x}_1^2\bar{z}_1 + \bar{x}_2^2\bar{z}_2 + \bar{x}_3^2\bar{z}_3 + \bar{x}_4^2\bar{z}_4 = 0 \\ \bar{x}_1\bar{y}_1\bar{z}_1 + \bar{x}_2\bar{y}_2\bar{z}_2 + \bar{x}_3\bar{y}_3\bar{z}_3 + \bar{x}_4\bar{y}_4\bar{z}_4 = 0 \end{cases}$$

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

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ \bar{x}_1 & \bar{x}_2 & \bar{x}_3 & \bar{x}_4 \\ \bar{y}_1 & \bar{y}_2 & \bar{y}_3 & \bar{y}_4 \\ \bar{x}_1^2 & \bar{x}_2^2 & \bar{x}_3^2 & \bar{x}_4^2 \\ \bar{x}_1\bar{y}_1 & \bar{x}_2\bar{y}_2 & \bar{x}_3\bar{y}_3 & \bar{x}_4\bar{y}_4 \end{pmatrix} \tag{22}$$

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

If all $\bar{x}_i$'s are equal, we have 4 points on a vertical line; the rank is 2 and the number of codewords is (see case H_3^0)

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

If only three $\bar{x}_i$'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 $\bar{x}_i$'s (for instance, $\bar{x}_1 = \bar{x}_2 \neq \bar{x}_3 = \bar{x}_4$), we can deduce $\bar{z}_1 + \bar{z}_2 = 0$, $\bar{z}_3 + \bar{z}_4 = 0$, and then

$$\begin{cases} \bar{z}_1(\bar{y}_1 - \bar{y}_2) + \bar{z}_3(\bar{y}_3 - \bar{y}_4) = 0 \\ \bar{x}_1\bar{z}_1(\bar{y}_1 - \bar{y}_2) + \bar{x}_3\bar{z}_3(\bar{y}_3 - \bar{y}_4) = 0 \end{cases},$$

but this system in the unknowns $\bar{y}_1 - \bar{y}_2, \bar{y}_3 - \bar{y}_4$ has determinant $\bar{z}_1\bar{z}_3(\bar{x}_3 - \bar{x}_1) \neq 0$, so that $\bar{y}_1 = \bar{y}_2$ and $\bar{y}_3 = \bar{y}_4$, which is impossible.

If only two $\bar{x}_i$'s are equal, say $\bar{x}_1 = \bar{x}_2$, we can show that we have $\bar{z}_1 + \bar{z}_2 = 0$, $\bar{z}_3 = 0, \bar{z}_4 = 0$ (as above), which is not admissible.

If we have all $\bar{x}_i$'s distinct, the submatrix

$$\begin{pmatrix} 1 & 1 & 1 & 1 \\ \bar{x}_1 & \bar{x}_2 & \bar{x}_3 & \bar{x}_4 \\ \bar{x}_1^2 & \bar{x}_2^2 & \bar{x}_3^2 & \bar{x}_4^2 \end{pmatrix}$$

has rank 3, but if the whole matrix (22) had rank 4 we could only have the zero solution, which is not admissible. Thus, (22) must have rank 3, that is, the $\bar{y}_i$'s and $\bar{x}_i\bar{y}_i$'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

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

Putting all together we get A_4, that is, the last part of Theorem 10.

3.5.4. Study of H_4^0

We count the number of words with weight $w = 5$. We have a linear system in $\bar{z}_i$ with a (6×5) 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

$$\begin{cases} xy = a + bx + cy + dx^2 \\ y^2 = e + fx + gy + hx^2. \end{cases}$$

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

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

Doing the computations we obtain the first part of Theorem 11.

3.5.5. Study of $\mathsf{H}_4^1, \mathsf{H}_4^2, \mathsf{H}_4^3$

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

$$\mathsf{H}_4^0 \supseteq \mathsf{H}_4^1 \supseteq \mathsf{H}_4^2 \supseteq \mathsf{H}_4^3 \supseteq \mathsf{H}_5^0$$

and the first and the last code have all the 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

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

Doing the computations we obtain the last part of Theorem 11.

4. Conclusions and open problems

The so-called first-phase codes have nice geometric properties that allow their study, as first realized in Pellegrini (2006) and Sala and Pellegrini (2006). 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 (Couvreur, 2012; Ballico and Ravagnani, 2014; Fontanari and Marcolla, 2015), 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: Pellegrini (2006) and Sala and Pellegrini (2006), in 2010 at *the Claude Shannon Institute WCC*, Cork (Ireland), in 2011 at the *Mzuni Math Workshop*, Mzuzu University (Malawi) and at WCC 2011 (Pellegrini et al., 2011).

The seminal idea behind our starting point (Proposition 1) was in the second author's PhD thesis (Pellegrini, in preparation), which was studied in deep and generalized in the first author Master's thesis and PhD thesis (Marcolla, 2008, 2013). The first two authors would like to thank their supervisor, the third author.

The authors would like to thank the anonymous referees for their insightful comments.

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 (Greuel et al., 2007; Bosma et al., 1997).

References

Augot, D., 1996. Description of the minimum weight codewords of cyclic codes by algebraic system. Finite Fields Appl. 2, 138–152.

Ballico, E., Ravagnani, A., 2014. On the geometry of hermitian one-point codes. J. Algebra 397, 499–514.

Bosma, W., Cannon, J., Playoust, C., 1997. The Magma algebra system I: the user language. In: Computational Algebra and Number Theory. London, 1993.

Couvreur, A., 2012. The dual minimum distance of arbitrary-dimensional algebraic–geometric codes. J. Algebra 350 (1), 84–107.

de Boer, M., Pellikaan, R., 1999. Gröbner bases for codes. In: Some Tapas of Computer Algebra. Springer, pp. 237–259.

Fitzgerald, J., Lax, R.F., 1998. Decoding affine variety codes using Gröbner bases. Des. Codes Cryptogr. 13 (2), 147–158.

Fontanari, C., Marcolla, C., 2015. On the geometry of small weight codewords of dual algebraic geometric codes. Int. J. Pure Appl. Math. 98 (3), 303–307.

Geil, O., 2008. Evaluation codes from an affine-variety codes perspective. In: Martinez-Moro, E., et al. (Eds.), Advances in Algebraic Geometry Codes. World Scientific, pp. 153–180.

Goppa, V.D., 1981. Codes on algebraic curves. Sov. Math. Dokl. 24, 170–172.

Goppa, V.D., 1988. Geometry and Codes. Math. Appl. (Sov. Ser.), vol. 24. Kluwer Academic Publishers Group, Dordrecht. Translated from Russian by N.G. Shartse.

Greuel, G.-M., Pfister, G., Schönemann, H., 2007. Singular 3.0. A computer algebra system for polynomial computations. http://www.singular.uni-kl.de. Centre for Computer Algebra, University of Kaiserslautern.

Hirschfeld, J.W.P., 1998. Projective Geometries over Finite Fields. Clarendon Press, Oxford.

Hirschfeld, J., Korchmáros, G., Torres, F., 2008. Algebraic Curves over a Finite Field. Princeton Univ. Press.

Høholdt, T., van Lint, J.H., Pellikaan, R., 1998. Algebraic geometry of codes. In: Pless, V.S., Huffman, W. (Eds.), Handbook of Coding Theory, vol. I, II. North-Holland, pp. 871–961.

Lax, R.F., 2012. Generic interpolation polynomial for list decoding. Finite Fields Appl. 18 (1), 167–178.

Marcolla, C., 2008. Parole di peso piccolo dei Codici Hermitiani. Master's thesis (laurea specialistica). University of Trento, Department of Mathematics.

Marcolla, C., 2013. On structure and decoding of Hermitian codes. PhD thesis. University of Trento, Department of Mathematics.

Marcolla, C., Orsini, E., Sala, M., 2012. Improved decoding of affine-variety codes. J. Pure Appl. Algebra 216 (7), 1533–1565.

Marcolla, C., Pellegrini, M., Sala, M., 2014. On the Hermitian curve and its intersections with some conics. Finite Fields Appl. 28, 166–187.

Mora, T., Orsini, E., 2009. Decoding cyclic codes: the Cooper philosophy. In: Sala, M., Mora, T., Perret, L., Sakata, S., Traverso, C. (Eds.), Gröbner Bases, Coding, and Cryptography. In: RISC Book Ser.. Springer, Heidelberg, pp. 69–91.

Pellegrini, M., 2006. On the weight distribution of Hermitian codes. In: Workshop D1: Groebner Bases in Cryptography, Coding Theory and Algebraic Combinatorics. Linz.

Pellegrini, M., in preparation. On the weight distribution of some Goppa AG codes. PhD thesis. University of Pisa.

Pellegrini, M., Marcolla, C., Sala, M., 2011. On the weights of affine-variety codes and some Hermitian codes. In: Proc. of WCC. 2011, Paris, pp. 273–282. http://hal.inria.fr/inria-00614257/en.

Ruck, H.G., Stichtenoth, H., 1994. A characterization of Hermitian function fields over finite fields. J. Reine Angew. Math. 457, 185–188.

Sala, M., 2007. Gröbner basis techniques to compute weight distributions of shortened cyclic codes. J. Algebra Appl. 6 (3), 403–404.

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

Seidenberg, A., 1974. Constructions in algebra. Trans. Am. Math. Soc. 197, 273–313.

Stichtenoth, H., 1993. Algebraic Function Fields and Codes. Universitext. Springer-Verlag, Berlin.

Vlăduţ, S.G., Manin, Y.I., 1984. Linear codes and modular curves. Itogi Nauki Tekh. Ser. Sovrem. Probl. Mat. Nov. Dostizh. 25, 209–257.