On the Hermitian curve and its intersections with some conics

On the Hermitian curve and its intersections with some conics

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

We classify completely the intersections of the Hermitian curve with parabolas in the affine plane. To obtain our results we employ well-known algebraic methods for finite fields and geometric properties of the curve automorphisms. In particular, we provide explicit counting formulas that have also applications to some Hermitian codes.

Keywords: Hermitian curve, intersection, parabola.

1 Introduction

Let q be a power of a prime. 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 is the best-known example of maximal curve and there is a vast literature on its properties, see [HKT08] for a recent survey.

Although a lot of research has been devoted to geometric properties of $\mathcal{H}$, we present in this paper a classification result, providing for any q the number of possible intersection points between any parabola and $\mathcal{H}$. With parabola we mean a curve $y = ax^2 + bx + c$, where $x, y \in \mathbb{F}_{q^2}$ and a, b, c are given with $a \neq 0$ and $a, b, c \in \mathbb{F}_{q^2}$. Moreover, we can characterize precisely the parabolas obtaining a given number of intersection points and we can count them. More precisely, given two curves X and Y lying in the affine plane $\mathbb{A}^2(\mathbb{F}_q)$ it is interesting to know the number of (affine plane) points that lie in both curves, disregarding multiplicity. We call this number *their planar intersection*.

Our main result is the following

Theorem A (Theorem 3.1 short version)**.** *The only possible planar intersections of $\mathcal{H}$ and a parabola are:*

- ✧ *for q odd* $\{0, 1, q-1, q, q+1, 2q-1, 2q\}$,
- ✧ *for q even* $\{1, q-1, q+1, 2q-1\}$.

For any possible planar intersection we have computed explicitly the exact number of parabolas sharing that value.

The paper is organized as follows:

- In Section 2 we introduce the definitions of norm and trace functions and some lemmas that we need to prove our main theorem (Theorem 3.1). Finally, we sketch our proving argument, that is, the use of the automorphism group for $\mathcal{H}$.
- In Section 3 we state and prove Theorem 3.1. The proof is divided in two main parts: in Subsection 3.1 we deal with the odd-characteristics case and in Subsection 3.2 we deal with the even-characteristics case.
- In Section 4 we show the relation between our results and a family of Hermitian codes.
- In Section 5 we draw some conclusions and propose some open problems.

2 Preliminary results

Let $\mathbb{F}_q$ be the finite field with q elements, where q is a power of a prime and let $\mathbb{F}_{q^2}$ be the finite field with q^2 elements. We call α a primitive element of $\mathbb{F}_{q^2}$, and we consider $\beta = \alpha^{q+1}$ as a primitive element of $\mathbb{F}_q$.

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 $x, y \in \mathbb{F}_{q^2}$. We recall that this curve has genus $g = \frac{q(q-1)}{2}$ and has $n = q^3$ $\mathbb{F}_{q^2}$-rational affine points and one point at infinity P_∞, so it has $q^3 + 1$ rational points over $\mathbb{F}_{q^2}$ [RS94].

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

Definition 2.1. *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*

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

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

Using these functions, we define the map $F_a : \mathbb{F}_{q^2} \to \mathbb{F}_q$ such that

$$F_a(x) = \mathrm{N}(x) - \mathrm{Tr}(ax^2). \tag{1}$$

We can note that the following property holds for the function F_a:

Lemma 2.2. *If $\omega \in \mathbb{F}_q$, then $F_a(\omega x) = \omega^2 F_a(x)$.*

Proof. Since $\omega \in \mathbb{F}_q$, we have $F_a(\omega x) = \mathrm{N}(\omega x) - \mathrm{Tr}(a(\omega x)^2) = \omega^{q+1}x^{q+1} - a^q\omega^{2q}x^{2q} - a\omega^2x^2 = \omega^2(x^{q+1} - a^qx^{2q} - ax^2) = \omega^2 F_a(x)$. □

2.1 Elementary results

Lemma 2.3. *Let $t \in \mathbb{F}_{q^2}^*$, then there is a solution of $x^{q-1} = t$ if and only if $\mathrm{N}(t) = 1$. In this case, $x^{q-1} = t$ has exactly $(q-1)$ distinct solutions in $\mathbb{F}_{q^2}$.*

Proof. This lemma is the Hilbert's Theorem 90 (see Theorem 6.1 of [Lan02]). □

Remark 2.4. We note that $4\mathrm{N}(a) = \mathrm{N}(2a)$ for any $a \in \mathbb{F}_{q^2}$.

Lemma 2.5. *If q is odd and $4\mathrm{N}(a) = 1$ then a is a square in $\mathbb{F}_{q^2}$.*

Proof. Let $a = \alpha^k$, so $4\mathrm{N}(a) = 1$ implies that $4\alpha^{k(q+1)} = 1$ i.e. $4\beta^k = 1$. Since 4 is a square in $\mathbb{F}_q$, we have $4 = \beta^{2t}$, that is, $\beta^{2t+k} = 1$ and so $2t + k \equiv 0 \mod q - 1$. Hence that k is even and a is a square. □

Lemma 2.6. *Let $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ such that $f(x) = 2ax - x^q$. Then the equation $f(x) = k$ has q distinct solutions if $k \in \mathrm{Im}(f)$, otherwise it has 0 solutions.*

Proof. Since f is $\mathbb{F}_q$-linear, our claim follows from standard results in linear algebra. □

Lemma 2.7. *Let $y = ax^2 + bx + \bar{c}$ and $y = ax^2 + bx + c$ be two parabolas. If $\mathrm{Tr}(\bar{c}) = \mathrm{Tr}(c)$, then the planar intersections between the Hermitian curve $\mathcal{H}$ and the parabolas are the same.*

Proof. From a set $\{y = ax^2+bx+\bar{c}\}\cap\mathcal{H}$ and another set $\{y = ax^2+bx+c\}\cap\mathcal{H}$ we obtain by direct substitution respectively $x^{q+1} = a^qx^{2q} + ax^2 + b^qx^q + bx + \mathrm{Tr}(\bar{c})$ and $x^{q+1} = a^qx^{2q} + ax^2 + b^qx^q + bx + \mathrm{Tr}(c)$. If $\mathrm{Tr}(\bar{c}) = \mathrm{Tr}(c)$, the two equations are identical. □

Finally, we recall the definition of *quadratic character* of $\mathbb{F}_q$.
Let q be odd, then

$$\eta(a) = \begin{cases} 1 & \text{if } a \equiv k^2 \mod q \\ -1 & \text{if } a \not\equiv k^2 \mod q \\ 0 & \text{if } a \equiv 0 \mod q. \end{cases}$$

Theorem 2.8. *Let $f(x) = ax^2 + bx + c \in \mathbb{F}_q[x]$ with q odd and $a \neq 0$. Let $d = b^2 - 4ac$, then*

$$\sum_{\gamma \in \mathbb{F}_q} \eta(f(\gamma)) = \begin{cases} -\eta(a) & \text{if } d \neq 0 \\ (q-1)\eta(a) & \text{if } d = 0. \end{cases}$$

Proof. See Theorem 5.48 of [LN97] □

2.2 Automorphisms of Hermitian curve

We consider an automorphism group $Aut(\mathcal{H}/\mathbb{F}_{q^2})$ of the Hermitian curve over $\mathbb{F}_{q^2}$. $Aut(\mathcal{H}/\mathbb{F}_{q^2})$ contains a subgroup Γ, such that any $\sigma \in \Gamma$ has the following form, as in [Xin95] and in Section 8.2 of [Sti93]:

$$\sigma \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} \epsilon x + \gamma \\ \epsilon^{q+1} y + \epsilon \gamma^q x + \delta \end{pmatrix}$$

with $(\gamma, \delta) \in \mathcal{H}$, $\epsilon \in \mathbb{F}_{q^2}^*$. Note that Γ is also a subset of the group of affine transformations preserving the set of $\mathbb{F}_{q^2}$-rational affine points of $\mathcal{H}$.
If we choose $\epsilon = 1$ we obtain the following automorphisms

$$\begin{cases} x \longmapsto x + \gamma \\ y \longmapsto y + \gamma^q x + \delta \end{cases} \qquad \text{with } (\gamma, \delta) \in \mathcal{H}, \tag{2}$$

that form a subgroup Λ with q^3 elements, see Section II of [Sti88].
The reason why we are interested in the curve automorphisms is the following. If we apply any σ to any curve $\mathcal{X}$ in the affine plane, then the planar intersections between $\sigma(\mathcal{X})$ and $\mathcal{H}$ will be the same as the planar intersections between $\mathcal{X}$ and $\mathcal{H}$. We recall that the number of planar intersection between two curves X and Y lying in the affine plane $\mathbb{A}^2(\mathbb{F}_q)$ is the number of (affine plane) points that lie in both curves, disregarding multiplicity. So, if we find out the number of intersections between $\mathcal{X}$ and $\mathcal{H}$, we will automatically have the number of intersection between $\sigma(\mathcal{X})$ and $\mathcal{H}$ for all $\sigma \in \Gamma$. This is convenient because we can isolate special classes of parabolas that act as representatives in the orbit $\{\sigma(\mathcal{X})\}_{\sigma \in \Gamma}$. These special types of parabolas may be easier to handle.

Note that if we apply (2) to $y = ax^2$, we obtain

$$y = ax^2 + x(2a\gamma - \gamma^q) + a\gamma^2 - \delta, \tag{3}$$

while if we apply (2) to $y = ax^2 + c$ we obtain

$$y = ax^2 + x(2a\gamma - \gamma^q) + a\gamma^2 - \delta + c. \tag{4}$$

In the general case, if we have $y = ax^2 + bx + c$ and apply the automorphism (2) we obtain

$$y = ax^2 + (2a\gamma - \gamma^q + b)x + a\gamma^2 + b\gamma - \delta + c. \tag{5}$$

To prove Theorem 3.1, we have to study two distinct cases depending on the field characteristic. Subsection 3.1 is devoted to the proof of Theorem 3.1 when the characteristic is odd, while Subsection 3.2 is devoted to the proof of Theorem 3.1 when the characteristic is even.

3 Intersection between Hermitian curve $\mathcal{H}$ and parabolas

We recall the definition of the Hermitian curve $\mathcal{H}$ on $\mathbb{F}_{q^2}$, i.e.

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

The number of planar intersection between two curves X and Y lying in the affine plane $\mathbb{A}^2(\mathbb{F}_q)$ may have applications for the codes constructed from X and Y. Regarding $\mathcal{H}$, it is interesting for coding theory applications [Cou11], [BR12a,BR12b,FM11] to consider an arbitrary parabola $y = ax^2 + bx + c$ over $\mathbb{F}_{q^2}$ and to compute their planar intersection. Moreover, it is essential to know precisely the number of parabolas having a given planar intersection with $\mathcal{H}$. Although nice partial results have been recently obtained in [DD10,DDK09] (where a much more general situation is treated), we present here for the first time a complete classification in the following theorem.

Theorem 3.1. *For q odd, the only possible planar intersections of $\mathcal{H}$ and a parabola are $\{0, 1, q-1, q, q+1, 2q-1, 2q\}$. For any possible planar intersection we provide in the next tables the exact number of parabolas sharing that value.*

$\#\mathcal{H}\cap$ parabola	0	1	$q-1$
# parabolas	$q^2(q+1)\frac{(q-1)}{2}$	$q^2(q+1)\frac{q(q-3)}{2}$	$q^2(q+1)\frac{q(q-1)^2}{2}$

$\#\mathcal{H}\cap$ parabola	q	$q+1$
# parabolas	$q^2(q+1)(q^2-q+1)$	$q^2(q+1)\frac{q(q-1)(q-3)}{2}$

$\#\mathcal{H}\cap$ parabola	$2q-1$	$2q$
# parabolas	$q^2(q+1)\frac{q(q-1)}{2}$	$q^2(q+1)\frac{(q-1)}{2}$

For q even, the only possible planar intersections of $\mathcal{H}$ and a parabola are $\{1, q-1, q+1, 2q-1\}$. For any possible planar intersection we provide in the next tables the exact number of parabolas sharing that value.

$\#\mathcal{H}\cap$ parabola	1	$q-1$
# parabolas	$q^3(q+1)(\frac{q}{2}-1)$	$q^3(q+1)(q-1)\frac{q}{2}$

$\#\mathcal{H}\cap$ parabola	$q+1$	$2q-1$
# parabolas	$q^3(q+1)(q-1)(\frac{q}{2}-1)$	$q^3(q+1)\frac{q}{2}$

3.1 Odd characteristics

In this subsection, q is always odd.

We provide now the sketch of the proof. Let $a, b, c \in \mathbb{F}_{q^2}$ and $a \neq 0$. We organize the proof in two main parts: in the first we analyze the intersection between $\mathcal{H}$ and parabola of type $y = ax^2 + c$ (Subsection 3.1.1) and in the second one we compute the number of intersection between $\mathcal{H}$ and the more general case $y = ax^2 + bx + c$ (Subsection 3.1.2) for nearly all cases. The last cases are dealt with a simple counting argument. For each of these subsections the proof is organized in several steps that are summarized in the following scheme.

1) $\mathcal{H} \cap \{\mathbf{y = ax^2 + c}\}$.
By intersecting $\mathcal{H}$ with $\{y = ax^2 + c\}$ we are led to consider the equation $F_a(x) = -\mathrm{Tr}(c)$, where $F_a(x)$ is as in (1), that is,

$$F_a(x) = a^q x^2 \left(x^{q-1} - \tfrac{1+\sqrt{\Delta}}{2a^q}\right)\left(x^{q-1} - \tfrac{1-\sqrt{\Delta}}{2a^q}\right) \text{ with}$$
$$\Delta = 1 - 4\mathrm{N}(a).$$

We call $\mathcal{A} := \mathcal{H} \cap \{y = ax^2 + c\}$ with a, c fixed. We are interested in the x position of points in $\mathcal{A}$ (that we call "solutions of $\mathcal{A}$"). That is, the number of the x's that verify the equation $F_a(x) = -\mathrm{Tr}(c)$, with a, c fixed.
We consider two subcases:

* $\mathrm{Tr}(c) = 0$. If
  - $\Delta = 0 \implies \mathcal{A}$ has q solutions.
  - $\Delta = 1 \implies \mathcal{A}$ has no solution.
  - $\Delta = z^2 \in \mathbb{F}_q \backslash \{0, 1\} \implies \begin{cases} z \in \mathbb{F}_q \implies \mathcal{A} \text{ has 1 solution.} \\ z \notin \mathbb{F}_q \implies \mathcal{A} \text{ has } 2q-1 \text{ solutions.} \end{cases}$

Now we apply the *automorphism* (2) to the parabola $y = ax^2 + c$ and we obtain $y = ax^2 + b'x + c'$, for some $b', c' \in \mathbb{F}_{q^2}$. We prove that when $\Delta \neq 0$, we have exactly q^3 distinct parabolas that share with $y = ax^2$ the planar intersection.

* $\mathrm{Tr}(c) \neq 0$. If
  - $\Delta = 0 \implies \begin{cases} \mathcal{A} \text{ has 0 solution.} \\ \mathcal{A} \text{ has } 2q \text{ solutions.} \end{cases}$ Both cases depend on a.
  - $\Delta = z^2 \in \mathbb{F}_q \backslash \{0, 1\} \implies \begin{cases} z \in \mathbb{F}_q \implies \mathcal{A} \text{ has } q+1 \text{ solutions.} \\ z \notin \mathbb{F}_q \implies \mathcal{A} \text{ has } q-1 \text{ solutions.} \end{cases}$

2) $\mathcal{H} \cap \{\mathbf{y = ax^2 + bx + c}\}$.
We apply the *automorphism* (2) to the parabola $y = ax^2 + bx + c$ and we obtain $y = ax^2 + b'x + c'$, for some $b', c' \in \mathbb{F}_{q^2}$. We consider two subcases:
   * $b' \neq 0$. If $4\mathrm{N}(a) = 1$, that is, $\Delta = 0$ we can write any such parabola as $y = a(x + v)^2$, where $v \in \mathbb{F}_{q^2}$ such that $v^q + 2av \neq 0$. So we have q points of intersection between $\mathcal{H}$ and $y = a(x + v)^2$, with a, v fixed.
   * $b' = 0$. Therefore, we apparent fall in the case 1). However, we actually dealing with different conditions of type $\mathrm{Tr}(c) = 0, \mathrm{Tr}(c) \neq 0$, $\Delta = 0$ and $\Delta \neq 0$.
   So we apply the *automorphism* (2) to the parabola $y = ax^2 + c'$ and we obtain $y = ax^2 + bx + \bar{c}$, for some $\bar{c} \in \mathbb{F}_{q^2}$. We want to understand *how many different parabolas* we can obtain when $\mathrm{Tr}(\bar{c}) \neq 0$. We divide two cases:
     - $\Delta = 0 \implies q^2(q + 1)$ possible parabolas (fixing a).
     - $\Delta = z^2 \in \mathbb{F}_q \backslash \{0, 1\} \implies q^3(q - 1)$ possible parabolas (fixing a).

3) Finally, we obtain the number of parabolas that have q intersections with the Hermitian curve by a simple counting argument.

3.1.1 Intersection between $\mathcal{H}$ and $y = ax^2 + c$

Intersecting a parabola of the form $y = ax^2 + c$ with the Hermitian curve, we obtain $x^{q+1} = a^q x^{2q} + ax^2 + \mathrm{Tr}(c)$ which is equivalent to

$$\mathrm{N}(x) - \mathrm{Tr}(ax^2) = F_a(x) = \mathrm{Tr}(c). \tag{6}$$

We have to study the number of solutions of (6). From this equation we get $a^q x^{2q} - x^{q+1} + ax^2 = -\mathrm{Tr}(c)$, that is,

$$x^2(a^q x^{2q-2} - x^{q-1} + a) = -\mathrm{Tr}(c). \tag{7}$$

Now we set $x^{q-1} = t$ and we factorize the polynomial $a^q t^2 - t + a$ in $\mathbb{F}_{q^2}[t]$, obtaining

$$t_{1,2} = \frac{1 \pm \sqrt{1 - 4\mathrm{N}(a)}}{2a^q} = \frac{1 \pm \sqrt{\Delta}}{2a^q}$$

where $\Delta = 1 - 4\mathrm{N}(a)$. So equation (7) becomes

$$a^q x^2 \left(x^{q-1} - \frac{1 + \sqrt{\Delta}}{2a^q} \right) \left(x^{q-1} - \frac{1 - \sqrt{\Delta}}{2a^q} \right) = -\mathrm{Tr}(c). \tag{8}$$

Since $\Delta \in \mathbb{F}_q$, there exists $z \in \mathbb{F}_{q^2}$ such that $\Delta = z^2$, and so equation (8) is in $\mathbb{F}_{q^2}[x]$.
Note that

$$\Delta = 0 \iff \mathrm{N}(2a) = 1.$$

So, in this special case, (8) becomes $a^q x^2 (x^{q-1} - 2a)^2 = -\mathrm{Tr}(c)$. We have proved the following lemma.

Lemma 3.2. *By intersecting a parabola $y = ax^2 + c$, where $\mathrm{N}(2a) = 1$, and the Hermitian curve, we obtain the following equation*

$$a^q x^2 (x^{q-1} - 2a)^2 = -\mathrm{Tr}(c).$$

Recall that α is a primitive element of $\mathbb{F}_{q^2}$ and $\beta = \alpha^{q+1}$ is a primitive element of $\mathbb{F}_q$.

Lemma 3.3. *Let $x = \alpha^j \beta^i$, with $j = 0, \ldots, q$ and $i = 0, \ldots, q-2$. Then*

- ✧ *If $4\mathrm{N}(a) \neq 1$, then the non-zero values $F_a(\alpha^j \beta^i)$ are all the elements of $\mathbb{F}_q^*$.*
- ✧ *If $4\mathrm{N}(a) = 1$, then the non-zero values $F_a(\alpha^j \beta^i)$ are half of the elements of $\mathbb{F}_q^*$.*

Proof. We recall that $F_a(x) = x^{q+1} - a^q x^{2q} - ax^2$. We fix an index j such that $F_a(\alpha^j) \neq 0$. The set of the values

$$\{F_a(\alpha^j \beta^i)\}_{0 \leq i \leq q-2} = \{\beta^{2i} F_a(\alpha^j)\}_{0 \leq i \leq q-2}$$

contains half of the elements of $\mathbb{F}_q^*$, since q is odd (and $\frac{q-1}{2}$ is an integer) and so $\beta^{2(\frac{q-1}{2})} = \alpha^{q^2-1} = 1$. In particular, if $F_a(\alpha^j)$ is a square then $\{\beta^{2i} F_a(\alpha^j)\}_{0 \leq i \leq q-2}$ are all squares of $\mathbb{F}_q^*$ (and vice-versa if it is a non-square).
Suppose that $F_a(1) = 1 - a^q - a$ is a square and let $\bar{x} = y + \gamma \in \mathbb{F}_{q^2}$, where $y \in \mathbb{F}_q$, $\gamma \neq 0$ and $\mathrm{Tr}(\gamma) = 0$. Then

$$\begin{aligned} F_a(\bar{x}) &= -a^q (y - \gamma)^2 + (y - \gamma)(y + \gamma) - a(y + \gamma)^2 \\ &= y^2 (1 - a^q - a) + 2\gamma y (a^q - a) - \gamma^2 (a^q + a + 1) := f_\gamma(y). \end{aligned}$$

Since $f_\gamma(y) \in \mathbb{F}_q[y]$, we can apply Theorem 2.8, where $d = 4\gamma^2(1 - 4\mathrm{N}(a)) = 4\gamma^2\Delta$.

- ✧ If $\Delta \neq 0$ we have $\sum_{\epsilon\in\mathbb{F}_q} \eta(f_\gamma(\epsilon)) = -\eta(1 - a^q - a) = -1$, that is, there exists at least a $y_1 \in \mathbb{F}_q$ such that $f_\gamma(y_1)$ is not a square. Let $\bar{x}_1 = y_1 + \gamma \in \mathbb{F}_{q^2}$, then $F_a(\bar{x}_1\beta^i)$ and $F_a(1\beta^i)$, varying $i = 0, \ldots, q-2$, are all elements of $\mathbb{F}_q^*$ (that are all non-squares and all squares respectively).
- ✧ If $\Delta = 0$, by Lemma 3.2, $F_a(x)$ becomes $-a^q x^2(x^{q-1} - 2a)^2$, so $\beta^{2i}F_a(\alpha^j) = -a^q\beta^{2i}(\alpha^{jq} - 2a\alpha^j)^2$ and they are half of the elements of $\mathbb{F}_q^*$. In particular if $-a^q$ is a square we obtain all squares of $\mathbb{F}_q^*$, vice-versa, if $\eta(-a^q) = -1$, we have all non-squares of $\mathbb{F}_q^*$.

□

Now we study the number of solutions of equation (6), analyzing two cases: when $\mathrm{Tr}(c) = 0$ and when $\mathrm{Tr}(c) \neq 0$.

- ∗ Case $\mathrm{Tr}(c) = 0$. By Lemma 2.7, it is enough to study the case $c = 0$, which is the intersection between $\mathcal{H}$ and $y = ax^2$. By (8) we have

$$a^q x^2 \left(x^{q-1} - \frac{1 + \sqrt{\Delta}}{2a^q}\right)\left(x^{q-1} - \frac{1 - \sqrt{\Delta}}{2a^q}\right) = 0.$$

  We must differentiate our argument depending on Δ. Recall that $\Delta \in \mathbb{F}_q$.

  - $\Delta = 0$. By Lemma 3.2, (8) becomes

$$a^q x^2(x^{q-1} - 2a)^2 = 0.$$

    So we have always one solution $x = 0$ and the solutions of $x^{q-1} = 2a$. Since $\mathrm{N}(2a) = 1$, by Lemma 2.3, the number of solutions of $x^{q-1} = 2a$ are $q - 1$. Therefore, in this case, we have q points of intersections between the parabola and the Hermitian curve $\mathcal{H}$.
    By condition on a, i.e. $\mathrm{N}(2a) = 1$, we have $(q + 1)$ distinct a's.
  - $\Delta = 1$. That is, $\mathrm{N}(2a) = 0 \iff a = 0$, which is impossible.
  - $\Delta \in \mathbb{F}_q \backslash \{0, 1\}$. We note that any element in $\mathbb{F}_q$ can always be written as z^2 with $z \in \mathbb{F}_{q^2}$. So let $\Delta = z^2$. In order to study the solutions of (8), we can consider the solutions of the following equations

$$x^{q-1} = \frac{1 \pm z}{2a^q}. \tag{9}$$

    By Lemma 2.3 we know that $x^{q-1} = \frac{1+z}{2a^q}$ has solutions if and only if $\mathrm{N}\left(\frac{1+z}{2a^q}\right) = 1$. Note that

$$\mathrm{N}\left(\frac{1+z}{2a^q}\right) = 1 \iff \frac{(1+z)^{q+1}}{1-z^2} = 1 \iff 1 - z = (1+z)^q \iff -z = z^q$$

We obtain the same result for $x^{q-1} = \frac{1-z}{2a^q}$.
If (9) has a solution x and $z \in \mathbb{F}_q$, then z simultaneously satisfies $z^q = z$ and $z^q = -z$. Since q is odd, this is possible only when $z = 0$, which implies $\Delta = 0$, which is not admissible.

Returning to count the intersection points, thanks to the previous discussion of the solution of (9), we have to consider two distinct cases:

- ✧ $z = z^q$, that is, $z \in \mathbb{F}_q$. Since $z \neq 0, 1$, there are $\frac{q-1}{2} - 1 = \frac{q-3}{2}$ possible values of z^2, and so we have $(q+1)\frac{q-3}{2}$ values of a. In this case, the parabola $y = ax^2 + c$ intersects $\mathcal{H}$ in only *one* point (with $x = 0$).
- ✧ $z = -z^q$. The equation $-z = z^q$ has only one solution in $\mathbb{F}_q$, so the other $q-1$ solutions are in $\mathbb{F}_{q^2}\backslash\mathbb{F}_q$. For such z, we have $2(q-1)+1 = 2q-1$ points of intersection. That is, $q-1$ solutions from equation $x^{q-1} = \frac{1-z}{2a^q}$, $q-1$ solutions from equation $x^{q-1} = \frac{1+z}{2a^q}$ and one point from $x = 0$.
  It is simple to verify that the number of z^2 such that $z \in \mathbb{F}_{q^2}\backslash\mathbb{F}_q$ is $\frac{q-1}{2}$. So we have $(q+1)\frac{q-1}{2}$ values of a for which we have exactly $2q-1$ points of intersection between $y = ax^2 + c$ and $\mathcal{H}$.

Now we apply the automorphism (2) and we want to compute how many different parabolas we can obtain. Applying (2) to $y = ax^2$ we obtain (3):

$$y = ax^2 + x(2a\gamma - \gamma^q) + a\gamma^2 - \delta.$$

For the moment, we restrict our counting argument to the case $\Delta \neq 0$. We note that if $\Delta \neq 0$, we have a maximal orbit, that is, all possible parabolas are distinct (there are q^3 because Γ has q^3 elements). In other words, we claim that it is impossible that we obtain two equal parabolas with $(\gamma, \delta) \neq (\bar{\gamma}, \bar{\delta})$. To prove that, we have to solve the following system:

$$\begin{cases} 2a\bar{\gamma} - \bar{\gamma}^q = 2a\gamma - \gamma^q \\ a\bar{\gamma}^2 - \bar{\delta} = a\gamma^2 - \delta \\ \gamma^{q+1} = \delta^q + \delta \\ \bar{\gamma}^{q+1} = \bar{\delta}^q + \bar{\delta} \\ 1 - 4a^{q+1} \neq 0. \end{cases}$$

However, $2a\bar{\gamma} - \bar{\gamma}^q = 2a\gamma - \gamma^q \iff 2a(\bar{\gamma} - \gamma) = \bar{\gamma}^q - \gamma^q = (\bar{\gamma} - \gamma)^q$. Raising the equation to the power of $q+1$, we obtain $(2a)^{q+1}(\bar{\gamma} - \gamma)^{q+1} = (\bar{\gamma} - \gamma)^{q^2+q}$, that is, $4a^{q+1}(\bar{\gamma} - \gamma)^q(\bar{\gamma} - \gamma) = (\bar{\gamma} - \gamma)(\bar{\gamma} - \gamma)^q$, which is equivalent to $4a^{q+1} = 1$. This is impossible, since $\Delta \neq 0$.
Hence, when $\Delta \neq 0$, we have exactly q^3 distinct parabolas that have the

same planar intersections with $\mathcal{H}$ as $y = ax^2$ has.

* Case $y = ax^2 + c$, with $\mathrm{Tr}(c) \neq 0$. As in previous case, we have to differentiate depending on Δ.
  - If $\Delta = z^2$ and $z \in \mathbb{F}_q$, we know that $F_a(x)$ vanishes only if $x = 0$. If $x \neq 0$, then by Lemma 3.3, $F_a(\beta^i\alpha^j) = \beta^{2i}F_a(\alpha^j) = t$ assumes every value of $\mathbb{F}_q^*$. But $x = \beta^i\alpha^j$ assumes $q^2 - 1$ distinct values, varying i and j. So every t is obtained $q + 1$ times ($F_a(x)$ is a polynomial of degree $q + 1$). Hence, the equation $F_a(x) = \mathrm{Tr}(c)$ has exactly $q + 1$ solutions.
  - If $\Delta = z^2$ and $z \in \mathbb{F}_{q^2}\backslash\mathbb{F}_q$, we know that $F_a(x) = 0$ has $2q - 1$ solutions. So there are exactly two distinct values of j such that $F_a(\alpha^j) = 0$, one for each equation $x^{q-1} = \frac{1\pm z}{2a^q}$ (to find the $q - 1$ solutions, we vary i). So every value in $\mathbb{F}_q^*$ is obtained $q - 1$ times. Hence, the equation $F_a(x) = \mathrm{Tr}(c)$ has exactly $q - 1$ solutions.
  - If $\Delta = 0$ we have $4a^{q+1} = 1$.
    So (1) can be written as $a^q x^2(x^{q-1} - 2a)^2 = -\mathrm{Tr}(c)$, that is,

    $$x^2(x^{q-1} - 2a)^2 = -4a\mathrm{Tr}(c) = -4a\beta^r \tag{10}$$

    for some fixed r with $1 \leq r \leq q - 1$.
    Note that (10) can be written as $f(x)^2 = -4a\mathrm{Tr}(c)$, where f is as in Lemma 2.6, that is, $f(x) = x^q - 2ax$.
    We note that $-4a\beta^r$ is always a square in $\mathbb{F}_{q^2}$. In fact $-4\beta^r$ is a square because it lies in $\mathbb{F}_q$, and also a is a square by Lemma 2.5. Let us write $-4a\beta^r = \alpha^{2h}$, so (10) becomes $x(x^{q-1} - 2a) = \pm\,\alpha^h$ where $0 \leq h \leq \frac{q^2-1}{2}$.
    We consider the "positive" case:

    $$f(x) = x^q - 2ax = \alpha^h. \tag{11}$$

    It is simple to prove that if x is a solution of equation (11), then $-x$ is a solution of the equation $x^q - 2ax = -\alpha^h$. So by Lemma 2.6 the equation $F_a(x) = \mathrm{Tr}(c)$ has 0 solutions if α^h is not in $\mathrm{Im}(f)$ or $2q$ solution if α^h is in $\mathrm{Im}(f)$.

3.1.2 Intersection between $\mathcal{H}$ and $y = ax^2 + bx + c$

We consider a parabola $y = ax^2 + bx + c$, apply the automorphism (2) and we obtain (5).
Note that, for any $k \in \mathbb{F}_{q^2}$,

$$2a\gamma - \gamma^q + b = k \implies 2ab^q + b = 2ak^q + k, \tag{12}$$

because $b^q = (k - 2a\gamma + \gamma^q)^q = k^q - \frac{1}{2a}\gamma^q + \gamma = k^q + \frac{1}{2a}(-\gamma^q + 2a\gamma) = k^q + \frac{1}{2a}(k - b)$.

A consequence is that $2a\gamma - \gamma^q + b = 0 \implies 2ab^q + b = 0$.

We consider two distinct cases $2a\gamma - \gamma^q + b = 0$ and $2a\gamma - \gamma^q + b \neq 0$.

$\boxed{2a\gamma - \gamma^q + b \neq 0.}$

Theorem 3.4. *Let $y = ax^2 + bx + c$ be a parabola with $2ab^q + b \neq 0$ and $\mathrm{N}(2a) = 1$. Then there exists γ such that for any δ, applying the automorphism (2), we obtain $y = ax^2 + (2a\gamma - \gamma^q + b)x + a\gamma^2 + b\gamma - \delta + c$, with $2a\gamma - \gamma^q + b \neq 0$. We can write any such parabola as $y = (ux + uv)^2$ where $a = u^2$ and $v^q + 2av \neq 0$.*

Proof. Because of (12) with $k \neq 0$ we have that, since $2ab^q + b \neq 0$, there exists γ such that $2a\gamma - \gamma^q + b \neq 0$.
Let $k \in \mathbb{F}_{q^2} \backslash \{0\}$ such that $2a\gamma - \gamma^q + b = k \neq 0$. By Lemma 2.6, if there exists at least one solution of $2a\gamma - \gamma^q = k - b$, then there exist q solutions. So we have at least q different γ's that verify the previous equation.
To prove that any parabola as in (5) can be written $y = (ux+uv)^2$ with $a = u^2$ and $v^q + 2av \neq 0$, we claim that it is sufficient to prove that the solutions of the following system contain all c's.

$$\begin{cases} 2a\gamma - \gamma^q + b = 2av \neq 0 \\ a\gamma^2 + b\gamma - \delta + c = av^2 \neq 0 \\ \gamma^{q+1} = \delta^q + \delta \\ 1 - 4a^{q+1} = 0 \end{cases} \tag{13}$$

In fact, system (13) is obtain as follows. We have the first two equations comparing $y = (ux + uv)^2$ and $y = ax^2 + (2a\gamma - \gamma^q + b)x + a\gamma^2 + b\gamma - \delta + c$. Note that by Lemma 2.5, $a = u^2$ is a square so $y = (ux + uv)^2 = a(x + v)^2$. The third equation denote that the point $(\gamma, \delta) \in \mathcal{H}$ and finally, the last equation is a necessary condition to verify this theorem, that is, $\mathrm{N}(2a) = 1$.

We are ready to show the desired property of (13)'s solutions. Using (12), we first observe that the first equation of (13) implies that $v^q + 2av \neq 0$. Indeed if we consider (12) with $k = 2av$, we have $0 \neq 2ab^q + b = 2ak^q + k = 2a(2av)^q + 2av = v^q + 2av$.
Now, we prove that (13) has q^2 different c's in its solutions, that is, all possible c's. From the automorphism point of view, it is enough to prove that the point (γ, δ) of $\mathcal{H}$ are in bijection with the c's contained in solutions of (13). Which means that two distinct automorphisms (of the considered type) sends the curve in two distinct curves.
Multiplying the first equation by γ we substitute $2a\gamma^2$ in the second equation

multiplied by 2 and, using the curve equation $\gamma^{q+1} = \delta^q + \delta$, we obtain

$$2c = 2av^2 + \delta - \delta^q - \gamma(2av + b). \tag{14}$$

Suppose by contradiction that there exist two points $(\gamma_1, \delta_1), (\gamma_2, \delta_2) \in \mathcal{H}$ such that $(\gamma_1, \delta_1) \neq (\gamma_2, \delta_2)$ but $c_1 = c_2$, where c_i are as in (14). Since $c_1 = c_2$, we would obtain

$$\gamma_1(2av + b) - \delta_1 + \delta_1^q = \gamma_2(2av + b) - \delta_2 + \delta_2^q. \tag{15}$$

On the other hand, if we raise (15) to the power of q and substitute γ_i^q with the first equation of (13), that is, $\gamma_i^q = 2a\gamma_i + b - 2av$ for $i = 1, 2$, we obtain

$$2a\gamma_1(2av + b)^q - \delta_1^q + \delta_1 = 2a\gamma_2(2av + b) - \delta_2^q + \delta_2. \tag{16}$$

Summing the equations (15) and (16) we obtain $\gamma_1[(2av+b)+2a(2av+b)^q] = \gamma_2[(2av + b) + 2a(2av + b)^q]$, that is, $\gamma_1 = \gamma_2$ if $(2av + b) + 2a(2av + b)^q \neq 0$. Note $(2av + b) + 2a(2av + b)^q = 2av + b + 4a^{q+1}v^q + 2ab^q = v^q + 2av + 2ab^q + b = 2(2ab^q + b) \neq 0$, where we use the last equation of (13), so it must be $\gamma_1 = \gamma_2$. However, if $\gamma_1 = \gamma_2$ then $\delta_1 = \delta_2$ by the second equation of (13), and this implies a contradiction. Therefore, for any two different points $(\gamma_1, \delta_1), (\gamma_2, \delta_2) \in \mathcal{H}$ we have that $c_1 \neq c_2$. To conclude, we show that we have q^2 different c's. By the second equation we have $c = \delta + av^2 - a\gamma^2 - b\gamma$. So, for any γ (and there are q possible γ's), there are q distinct δ's (by the curve equation). □

Theorem 3.5. *Let $a, v \in \mathbb{F}_{q^2}$ such that $\mathrm{N}(2a) = 1$ and $v^q + 2av \neq 0$. Then the Hermitian curve $\mathcal{H}$ intersects the parabola $y = a(x + v)^2$ in q points.*

Proof. We have to solve the system

$$\begin{cases} y = (ux + uv)^2 \\ x^{q+1} = y^q + y \end{cases} \implies x^{q+1} = (ux + uv)^{2q} + (u + uv)^2$$

By a change of variables $z = ux + uv$, we obtain $(\frac{z-uv}{u})^{q+1} = z^{2q} + z^2$, so we have

$$-(uv)z^q - (uv)^q z + (uv)^{q+1} = u^{q+1}z^{2q} + u^{q+1}z^2 - z^{q+1} = u^{q+1}(z^q - 2u^{q+1}z)^2.$$

Since $\mathrm{N}(2a) = 1$ and $a = u^2$, we have $u^{q+1} = \pm\frac{1}{2}$ and so

$$\frac{1}{2}(z^q - z)^2 = \mathrm{N}(uv) - \mathrm{Tr}(z(uv)^q) \tag{17}$$

$$-\frac{1}{2}(z^q + z)^2 = \mathrm{N}(uv) - \mathrm{Tr}(z(uv)^q) \tag{18}$$

We consider two cases:

- ✧ If $u^{q+1} = \frac{1}{2}$, we claim that if $z^q - z \neq 0$, then $(z^q - z)^2$ is not a square in $\mathbb{F}_q$. In fact, suppose by contradiction that $(z^q - z)^2 = \beta^{2r}$, then $z^q - z = \beta^r \in \mathbb{F}_q$ but also $z^q + z \in \mathbb{F}_q$, so $-2z \in \mathbb{F}_q \iff z \in \mathbb{F}_q$ and so $z^q - z = 0$, which is impossible.
- ✧ If $u^{q+1} = -\frac{1}{2}$, we can note that $(z^q + z)^2$ is a square in $\mathbb{F}_q$, because $z^q + z \in \mathbb{F}_q$.

Let $t = \mathrm{N}(uv) - \mathrm{Tr}(z(uv)^q)$. So $t \in \mathbb{F}_q$. Due to (17) we have $2t = (z^q - z)^2$, while (18) becomes $-2t = (z^q + z)^2$.

When $u^{q+1} = \frac{1}{2}$, we have $\frac{q-1}{2}$ values of t (that are all the non-squares) and $t = 0$, whereas when $u^{q+1} = -\frac{1}{2}$, we have $\frac{q-1}{2}$ values of t (that are all the squares) and $t = 0$.
Now we consider separately the cases $t = 0$ and $t \neq 0$.

- ✧ We claim that if $t = 0$ and $u^{q+1} = \pm\frac{1}{2}$ then $z \in \mathbb{F}_q$. Whereas if $t = 0$ and $u^{q+1} = -\frac{1}{2}$ then $z \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. We show only the case $u^{q+1} = \frac{1}{2}$. With these assumptions (17) becomes

$$-(uv)z^q - (uv)^q z + (uv)^{q+1} = 0 \iff z = \frac{(uv)^{q+1}}{(uv)^q + uv}.$$

  We can note that since $v^q + 2av \neq 0$, then $(uv)^q + uv \neq 0$. In fact, suppose that $v^q + 2av = 0$, then $(uv)^q + uv = -\frac{1}{2u}2av + uv = 0$.
  We have to verify that $z^q = z$. Indeed $z^q = \frac{(uv)^{q+1}}{uv+(uv)^q} = z$.
  Similar computations (here omitted) show the case $u^{q+1} = -\frac{1}{2}$.

- ✧ We claim that if $t \neq 0$ and $u^{q+1} = \pm\frac{1}{2} \implies z \notin \mathbb{F}_q$. With these assumptions, we show only the case $u^{q+1} = \frac{1}{2}$. We have $(z^q - z)^2 = 2t = \alpha^{2r}$, that is, $z^q = z \pm \alpha^r$. Now we substitute z^q in $-(uv)z^q - (uv)^q z + (uv)^{q+1} = t$ and we obtain $-(uv)(\pm\alpha^r + z) - (uv)^q z + (uv)^{q+1} = \frac{1}{2}\alpha^{2r}$, that is,

$$z = \frac{(uv)^{q+1} - \frac{1}{2}\alpha^{2r} \mp uv\alpha^r}{\mathrm{Tr}(uv)} \tag{19}$$

  We can note that $\alpha^{qr} = -\alpha^r$, in fact $2t = \alpha^{2r} \in \mathbb{F}_q$, so $(\alpha^{2r})^q = \alpha^{2r}$, that is, $\alpha^{rq} = \pm\alpha^r$ but $\alpha^r \notin \mathbb{F}_q$ (since $2t$ is not a square in $\mathbb{F}_q$) so $\alpha^{qr} = -\alpha^r$. We have thus proved

$$z = \frac{(uv)^{q+1} - \frac{1}{2}\alpha^{2r} \mp uv\alpha^r}{\mathrm{Tr}(uv)} \text{ and } z^q = \frac{(uv)^{q+1} - \frac{1}{2}\alpha^{2r} \pm (uv)^q\alpha^r}{\mathrm{Tr}(uv)}$$

  Now we have to verify that the two z's as in (19) are solutions of (17).

We have $z^q - z = \pm\alpha^r$ and $\mathrm{N}(uv) - \mathrm{Tr}(z(uv)^q) = t$. So

$$\pm\alpha^r = z^q - z \iff \pm\mathrm{Tr}(uv)\alpha^r = \pm(uv)^q\alpha^r \pm uv\alpha^r$$

and

$$\begin{aligned}
&(uv)^{q+1} - z(uv)^q - z^q(uv) = t \\
\iff &(uv)^{q+1}\mathrm{Tr}(uv) - (uv)^q((uv)^{q+1} - \tfrac{1}{2}\alpha^{2r} \mp uv\alpha^r) + \\
&-uv((uv)^{q+1} - \tfrac{1}{2}\alpha^{2r} \pm uv\alpha^r) = \mathrm{Tr}(uv)t \\
\iff &(uv)^{q+1}\mathrm{Tr}(uv) + t\,\mathrm{Tr}(uv) - (uv)^{2q+1} - (uv)^{q+2} = \mathrm{Tr}(uv)t \\
\iff &(uv)^{q+1}\mathrm{Tr}(uv) - (uv)^{2q+1} - (uv)^{q+2} = 0.
\end{aligned}$$

So the z's are solutions of (17).
Similar computations (omitted here) show the case $u^{q+1} = -\frac{1}{2}$.

Therefore, we have two solutions for any t not a square in $\mathbb{F}_q^*$ and we have only one solution when $t = 0$. That is, we get a total of $2 \cdot \frac{q-1}{2} + 1 = q$ intersections. The same holds for the case with $u^{q+1} = -\frac{1}{2}$. □

Now we consider the second case.

$$\boxed{2a\gamma - \gamma^q + b = 0.}$$

We note that if $2a\gamma - \gamma^q + b = 0$ then $2ab^q + b = 0$, and so (5) is actually $y = ax^2 + \bar{c}$, where $\bar{c} = a\gamma^2 + b\gamma - \delta + c \in \mathbb{F}_{q^2}$. With abuse of notation, we will write $\bar{c} = c$, that is, $y = ax^2 + c$. Now we apply the automorphism (2) to the parabola $y = ax^2 + c$ and we obtain (4).

We study two different cases: if

* $\Delta \neq 0$, the parabolas in (4) are all distinct.

  The number of values of c such that $\mathrm{Tr}(c) \neq 0$ are exactly $q^2 - q$, but we must be careful and not count twice the same parabola. In particular, if two parabolas share a and b, then they are in the same orbit if $\mathrm{Tr}(c) = \mathrm{Tr}(c')$. So we must consider only one of these for any non-zero $\mathrm{Tr}(c)$. Thus there are $q - 1$ values.

Summarizing:

- If $\Delta = z^2$ and $z \in \mathbb{F}_q$ (and $\mathrm{Tr}(c) \neq 0$), then the number of parabolas with $q + 1$ intersections is

$$\underbrace{(q+1)\frac{q-3}{2}}_{a}\underbrace{q^3(q-1)}_{b,c} = \frac{1}{2}q^3(q^2-1)(q-3).$$

- If $\Delta = z^2$ and $z^q + z = 0$ (and $\mathrm{Tr}(c) \neq 0$), then the number of parabolas with $q-1$ intersections is

$$\underbrace{(q+1)\frac{q-1}{2}}_{a}\underbrace{q^3(q-1)}_{b,c} = \frac{1}{2}q^3(q+1)(q-1)^2.$$

$*$ $\Delta = 0$, that is, $4a^{q+1} = 1$, we want to understand how many different parabolas of the type $y = ax^2 + bx + \bar{c}$ (with a fixed) we can obtain. So we have to study the number of pairs $(b, \bar{c})$.

We note that

$$\mathrm{Tr}(\bar{c}) = a^q b^2 + \mathrm{Tr}(c). \tag{20}$$

In fact

$$\begin{aligned}\mathrm{Tr}(\bar{c}) &= (a\gamma^2 - \delta)^q + a\gamma^2 - \delta + \mathrm{Tr}(c)\\ &= (a\gamma^2)^q + a\gamma^2 - \gamma^{q+1} + \mathrm{Tr}(c) = a^q\gamma^2(\gamma^{q-1} - 2a)^2 + \mathrm{Tr}(c).\end{aligned}$$

Let $\mathrm{Tr}(c) = k$, with $k \in \mathbb{F}_q^*$. Let us consider two distinct cases:

- $\mathrm{Tr}(c) = \mathrm{Tr}(\bar{c})$. By (20) we have that $\mathrm{Tr}(c) = \mathrm{Tr}(\bar{c}) \iff b = 0$.
  So the number of pairs $(0, \bar{c})$ are exactly $q^2 - q$, because they correspond to all $\bar{c} \in \mathbb{F}_{q^2}$ such that $\mathrm{Tr}(\bar{c}) \neq 0$.
- $\mathrm{Tr}(c) \neq \mathrm{Tr}(\bar{c})$. Then $\mathrm{Tr}(\bar{c}) = a^q b^2 + k$.
  Since $b = 2a\gamma - \gamma^q$, then, by considering all possible γ's, we obtain $q-1$ distinct b's.
  In fact, we can consider the function $f : \mathbb{F}_{q^2} \to \mathbb{F}_{q^2}$ such that $f(\gamma) = 2a\gamma - \gamma^q$. By Lemma 2.6, for any $t \in \mathrm{Im}(f)$, the equation $f(\gamma) = t$ has q distinct solutions.
  Since we are interested in the case $b \neq 0$, we have $\frac{(q^2-q)}{q} = q - 1$ different b's. We can note that if b is a solution of the equation $2a\gamma - \gamma^q = 0$, then $-b$ is also a solution.
  Since we are interested in the pairs $(b^2, \bar{c})$, we note that we have to consider the equation $\mathrm{Tr}(\bar{c}) = a^q b^2 + k$, so the pairs $(b^2, \bar{c})$ are exactly $\frac{q-1}{2}(q^2 - q)$. In fact there are $\frac{q-1}{2}$ distinct b^2's and for any pairs (b^2, k) we have exactly q distinct $\bar{c}$'s. While the possible k's are exactly $q-1$ (because $\mathrm{Tr}(c) \neq 0$).
  All possible pairs $(b, \bar{c})$ are $2\frac{q-1}{2}(q^2 - q) = (q-1)(q^2 - q)$.

We fix a and we obtain exactly $(q-1)(q^2-q) + q^2 - q = q^2(q-1)$ parabolas of the type $y = ax^2 + bx + \bar{c}$.

In conclusion if $\Delta = 0$ and $\mathrm{Tr}(c) \neq 0$, then we have $q^2(q+1)\frac{q-1}{2}$ parabolas with $2q$ or 0 intersections.

The last type of parabolas cannot be easily counted and so we obtain their number by difference.

Claim 3.6. *The number of parabolas that have q intersections with the Hermitian curve $\mathcal{H}$ is $q^2(q+1)(q^2-q+1)$.*

Proof. The number of total parabolas is $q^4(q^2-1)$. By summing all parabolas that we already counted we obtain

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

$$=q^2(q+1)(q-1+q^2(q-2)).$$

So the number of parabolas that have q intersections with $\mathcal{H}$ is

$$q^4(q^2-1)-q^2(q+1)(q-1+q^2(q-2))=$$

$$q^2(q+1)(q^2(q-1)-q+1-q^2(q-2))=q^2(q+1)(q^2-q+1).$$

□

We have proved the following theorems, depending on the two conditions $\mathrm{Tr}(c)=0$ or $\mathrm{Tr}(c)\neq 0$.

Theorem 3.7. *Let q be odd. A parabola $y=ax^2+c$ with $\mathrm{Tr}(c)=0$ intersects the Hermitian curve $\mathcal{H}$ in $2q-1, q$ or 1 points.*
Moreover, we have

$(q+1)\frac{q-1}{2}q^3$ *parabolas that intersect $\mathcal{H}$ in $2q-1$ points.*

$q^2(q+1)(q^2-q+1)$ *parabolas that intersect $\mathcal{H}$ in q points.*

$(q+1)\frac{q-3}{2}q^3$ *parabolas that intersect $\mathcal{H}$ in one point.*

Theorem 3.8. *Let q be odd. A parabola $y=ax^2+c$ with $\mathrm{Tr}(c)\neq 0$ intersects the Hermitian curve $\mathcal{H}$ in $2q, q+1, q-1$ or 0 points.*
Moreover, we have

$q^2(q+1)\frac{q-1}{2}$ *parabolas that intersect $\mathcal{H}$ in $2q$ points.*

$q^3(q+1)(q-1)\frac{q-3}{2}$ *parabolas that intersect $\mathcal{H}$ in $q+1$ points.*

$q^3(q+1)\frac{(q-1)^2}{2}$ *parabolas that intersect $\mathcal{H}$ in $q-1$ points.*

$q^2(q+1)\frac{q-1}{2}$ *parabolas that intersect $\mathcal{H}$ in 0 point.*

Therefore, by Theorem 3.7 and Theorem 3.8, we obtain the first half of Theorem 3.1.

3.2 Even characteristics

In this subsection, q is always even.

We claim that it is enough to consider just two special cases: $y = ax^2$ and $y = ax^2 + c$. Before studying these two cases, we consider the following lemma.

Lemma 3.9. *Let $x = \alpha^j \beta^i$, with $j = 0, \ldots, q$ and $i = 0, \ldots, q-2$; then the values $F_a(\alpha^j \beta^i)$ that are not zero are all the elements of $\mathbb{F}_q^*$.*

Proof. Fixing an index j, by Lemma 2.2 we have $F_a(\alpha^j \beta^i) = \beta^{2i} F_a(\alpha^j)$. If $F_a(\alpha^j) = 0$ we have finished, otherwise $\beta^{2i} F_a(\alpha^j)$ are all elements of $\mathbb{F}_q^*$, because also β^2 is a primitive element of $\mathbb{F}_q$. □

We divide the study into two parts.

∗ Case $y = ax^2$. We intersect $\mathcal{H}$ with $y = ax^2$ and we obtain

$$x^2(a^q x^{2q-2} - x^{q-1} + a) = 0. \tag{21}$$

We set $x^{q-1} = t$ and we have to solve the equation $a^q t^2 - t + a = 0$. Setting $z = ta^q$ we obtain

$$z^2 + z + a^{q+1} = 0.$$

It is known that this equation has solutions in a field of characteristic even if and only if $\mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_{q^2}}(a^{q+1}) = 0$ (by special case of Artin - Schreier Theorem, see Theorem 6.4 of [Lan02]). To show that this latter condition holds, observe first that when $\delta \in \mathbb{F}_q$ and q is even, we have $\mathrm{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^2}}(\delta) = 0$. Second, observe that $\mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_{q^2}}(\cdot) = \mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_q}(\mathrm{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^2}}(\cdot))$. Then we can write

$$\mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_{q^2}}(a^{q+1}) = \mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_q}(\mathrm{Tr}_{\mathbb{F}_q}^{\mathbb{F}_{q^2}}(a^{q+1})) = \mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_q}(0) = 0.$$

We also have $\mathrm{N}(t) = 1$, in fact $t^{q+1} = (x^{q-1})^{q+1} = 1$. Then we have

$$z^{q+1} = \mathrm{N}(z) = \mathrm{N}(a^q) = a^{q^2+q} = a^{q+1} = \mathrm{N}(a)$$

and so the equation becomes $z^2 + z + z^{q+1} = 0$. Since $t \neq 0, z \neq 0$, then we must have $z^q + z = 1$. We can note that, since $a^{q+1} \in \mathbb{F}_q$, then it is possible to compute its trace from $\mathbb{F}_q$ to $\mathbb{F}_2$, and we obtain

$$\mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_q}(a^{q+1}) = \mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_q}(z^{q+1}) = \mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_q}(z^2+z) = z+z^2+z^2+z^4+\ldots+z^{q/2}+z^q = z+z^q.$$

If it is equal to 0, we have a contradiction, then there is not any solution $x \in \mathbb{F}_{q^2}$. On the other hand if it is equal to 1, then we have solutions.

When the solutions exist, since $z^{q+1} = a^{q+1}$, a solution z is $a\alpha^{j(q-1)}$, for some j, and the other is $z + 1$, which we can write as $a\alpha^{j'(q-1)}$. From

each of these we have the corresponding $t = (\frac{\alpha^j}{a})^{q-1}$ and so the x's are $\frac{\alpha^{j+i(q+1)}}{a} = \frac{\alpha^j\beta^i}{a}$ and $\frac{\alpha^{j'+i(q+1)}}{a} = \frac{\alpha^{j'}\beta^i}{a}$, with $i = 0, \dots, q-2$.

By denoting $A = a^{q+1}$, we summarize the two distinct cases:

- If $\mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_q}(A) = 0$, then equation (21) has only *one* solution. On the other hand, $\mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_q}(A) = 0$ is satisfied by $q/2$ values for A, one of which is $a = 0$, which is impossible. So only $\frac{q}{2}-1$ values are actually possible for A, each of them having $q+1$ solutions to the equation $a^{q+1} = A$. Therefore, the total number of values for a is $(\frac{q}{2}-1)(q+1)$.
- If $\mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_q}(A) = 1$, then equation (21) has $2q-1$ solutions. This happens for $\frac{q}{2}$ values of A, so the possible values of a are $\frac{q}{2}(q+1)$.

As in the odd case, we apply the automorphism (2) to the parabolas of type $y = ax^2$ and we have that distinct automorphisms generate distinct parabolas. We omit the easy adaption of our earlier proof.
We have proved the following theorem:

Theorem 3.10. *The Hermitian curve $\mathcal{H}$ and the parabola $y = ax^2$ intersect in either one point or $2q-1$ points.*
Moreover, from the application of (2) to these parabolas, we obtain:

$q^3(\frac{q}{2}-1)(q+1)$ *parabolas with one point of intersection with $\mathcal{H}$.*
$q^3\frac{q}{2}(q+1)$ *parabolas with $2q-1$ points of intersection with $\mathcal{H}$.*

* Case $y = ax^2 + c$ with $\mathrm{Tr}(c) \neq 0$. We consider the equation (1). We divide the problem into two parts:

- If $\mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_q}(a^{q+1}) = 0$, we know that $F_a(x)$ is equal to zero only for $x = 0$. If $x \neq 0$, then by Lemma 3.9 if we fix j we have that $F_a(x) = F_a(\alpha^j\beta^i) = \beta^{2i}F_a(\alpha^j)$ are all the elements of $\mathbb{F}_q^*$. But j can assume $q+1$ distinct values, so any value of $\mathbb{F}_q^*$ can be obtained $q+1$ times. So, the equation $F_a(x) = \mathrm{Tr}(c)$ has exactly $q+1$ solutions.

- If $\mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_q}(a^{q+1}) = 1$, $F_a(x) = 0$ has $2q-1$ solutions. So, if we fix an index j, the values of $F_a(\alpha^j\beta^i) = \beta^{2i}F_a(\alpha^j)$ are all equal to zero or are all the elements of $\mathbb{F}_q^*$. There are exactly two distinct values of j that give zero, so any non-zero value of $\mathbb{F}_q$ can be obtained $q-1$ times. So, the equation $F_a(x) = \mathrm{Tr}(c)$ has exactly $q-1$ solutions.

We apply the automorphism (2) to the parabola $y = ax^2 + c$ and we obtain (4). These are all distinct and different from those of Theorem 3.10, because the planar intersection of $\mathcal{H}$ and the previous parabolas are different. The number of values of c such that $\mathrm{Tr}(c) \neq 0$ is exactly $q^2 - q$, but we must be careful and not count twice the same parabola. In particular, if two parabolas share a and b, then they are in the same orbit if $\mathrm{Tr}(c) = \mathrm{Tr}(\bar{c})$. So we must consider only one of these for any non-zero

value of $\mathrm{Tr}(c)$. These are $q-1$ of these values.
Summarizing, we have proved the following theorem:

Theorem 3.11. *The Hermitian curve $\mathcal{H}$ and the parabola $y = ax^2 + c$ with $\mathrm{Tr}(c) \neq 0$ intersect in either $q+1$ or $q-1$ points.*
Moreover, from the application of (2) to these parabolas, we obtain:

$q^3(\frac{q}{2}-1)(q+1)(q-1)$ *parabolas (with* $\mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_q}(a^{q+1}) = 0$*) with $q+1$ points of intersection with $\mathcal{H}$.*
$q^3\frac{q}{2}(q+1)(q-1)$ *parabolas (with* $\mathrm{Tr}_{\mathbb{F}_2}^{\mathbb{F}_q}(a^{q+1}) = 1$*) with $q-1$ points of intersection with $\mathcal{H}$.*

By summing all parabolas that we have found in Theorem 3.10 and Theorem 3.11, we obtain

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

Since this is exactly the total number of the parabolas, this means that we considered all parabolas, and so we obtain the second half of Theorem 3.1.

4 Applications to coding theory

The results present in this paper do allow the explicit determination of at least one weight for some Hermitian codes.

We consider a Hermitian code as a special case of affine-variety 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 $R = \mathbb{F}_{q^2}[x,y]/I$. Let $\mathcal{V}(I) = \{P_1, \ldots, P_n\}$, where $n = q^3$. We consider the *evaluation map* defined as follows:

$$\begin{aligned} \phi : R &\longrightarrow (\mathbb{F}_{q^2})^n \\ f &\longmapsto (f(P_1), \ldots, f(P_n)). \end{aligned}$$

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: $C(I,L) = \mathrm{Span}_{\mathbb{F}_{q^2}}\langle \phi(\mathcal{B}_{m,q})\rangle$ 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.

$$H = \begin{pmatrix} f_1(P_1) & \dots & f_1(P_n) \\ \vdots & \ddots & \vdots \\ f_k(P_1) & \dots & f_k(P_n) \end{pmatrix} \text{ where } \mathcal{B}_{m,q} = \{f_1, \dots, f_k\}.$$

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.

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

Table 1
The four phases of Hermitian codes

In the remainder of this section we focus on the first phase. This phase can be characterized by the condition $d \le q$. First-phase Hermitian codes can be either *edge codes* or *corner codes*, as explained below.

Definition 4.1. *Let $2 \le d \le q$ and let $1 \le j \le d-1$.*
Let $L_0^d = \{1, x, \dots, x^{d-2}\}, L_1^d = \{y, xy, \dots, x^{d-3}y\}, \dots, L_{d-2}^d = \{y^{d-2}\}$.
Let $l_1^d = x^{d-1}, \dots, l_j^d = x^{d-j}y^{j-1}$.

- ✧ *If $\mathcal{B}_{m,q} = L_0^d \sqcup \cdots \sqcup L_{d-2}^d$, then we say that $C(m,q)$ is a **corner code** and we denote it by H_d^0.*
- ✧ *If $\mathcal{B}_{m,q} = L_0^d \sqcup \cdots \sqcup L_{d-2}^d \sqcup \{l_1^d, \dots, l_j^d\}$, 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 4.2. *Let $2 \leq d \leq q$, $1 \leq j \leq d-1$. Then*

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

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).

A result present in [MPS12] related to intersection between parabola and $\mathcal{H}$ is in the following theorem.

Theorem 4.3. *The number of words of weight 4 of a corner code H_3^0 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_3^1 is:

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

*Where N_k is the number of **parabolas** and non-vertical lines that intersect $\mathcal{H}$ in exactly k points.*
The number of words of weight 4 of an edge code H_3^2 is:

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

Proof. See Theorem 4.13 of [MPS12]. □

Since the intersections between $\mathcal{H}$ and the lines are easy to compute, to determine N_k in previous theorem it is enough to apply Theorem 3.1.

5 Conclusions and open problems

Apparently, there are two natural generalizations of our work:

- The first is to investigate the planar intersection of $\mathcal{H}$ with other conics. Unfortunately, this is not so easy as it seems. The case with parabolas is manageable because they intersect the curve in a tangency double point at infinity. In the general conics case, we will not have this help from the geometry and we will not be able to replicate many explicit computations we have done in our lemmas. Therefore, if someone wants to investigate the general case, he will need some extra (non-trivial) ideas.

- The second is to investigate the planar intersections of parabolas and other curves. The natural candidates are the norm-trace curves [Gei03], which share many properties with the Hermitian curve.

In both cases, the investigation is not only interesting in itself, but it is likely to shed light on the weight distribution of some affine-variety codes.

Acknowledgements

This work was partially presented in 2012 at the PhD School on Gröbner bases, curves, codes and cryptography (Trento) and in 2013 at Effective Methods in Algebraic Geometry, MEGA [MPS13].

Previous results were present in the first author's PhD thesis [Mar13].

The first two authors would like to thank their supervisor, the third author.

For interesting discussions, the authors would like to thank: M. Giulietti, T. Mora and M. Pizzato.

References

[BR12a] E. Ballico and A. Ravagnani, *On Goppa codes on the Hermitian curve*, Arxiv preprint arXiv:1202.0894 (2012).

[BR12b] _____, *On the geometry of Hermitian one-point codes*, Arxiv preprint arXiv:1203.3162 (2012).

[Cou11] A. Couvreur, *The dual minimum distance of arbitrary-dimensional algebraic–geometric codes*, Journal of Algebra (2011).

[DD10] G. Donati and N. Durante, *On the intersection of a Hermitian curve with a conic*, Designs, Codes and Cryptography **57** (2010), no. 3, 347–360.

[DDK09] G. Donati, N. Durante, and G. Korchmaros, *On the intersection pattern of a unital and an oval in PG (2, q2)*, Finite Fields and Their Applications **15** (2009), no. 6, 785–795.

[FM11] C. Fontanari and C. Marcolla, *On the geometry of small weight codewords of dual algebraic geometric codes*, Arxiv preprint arXiv:1104.1320 (2011).

[Gei03] O. Geil, *On codes from norm-trace curves*, Finite Fields Appl. **9** (2003), 351–371.

[HKT08] J.W.P. Hirschfeld, G. Korchmáros, and F. Torres, *Algebraic curves over a finite field*, Princeton Univ Pr, 2008.

[HvLP98] T. Høholdt, J. H. van Lint, and R. Pellikaan, *Algebraic geometry of codes*, Handbook of coding theory, Vol. I, II (V. S. Pless and W.C. Huffman, eds.), North-Holland, 1998, pp. 871–961.

[Lan02] S. Lang, *Algebra revised third edition*, Springer-Verlag, 2002.

[LN97] R. Lidl and H. Niederreiter, *Finite fields*, Encyclopedia of Mathematics and its Applications, Cambridge University Press, 1997.

[Mar13] C. Marcolla, *On structure and decoding of Hermitian codes*, Ph.D. thesis, University of Trento, 2013.

[MPS12] C. Marcolla, M. Pellegrini, and M. Sala, *On the Hermitian curve, its intersections with some conics and their applications to affine-variety codes and Hermitian codes*, arXiv preprint arXiv:1208.1627 (2012).

[MPS13] C. Marcolla, M. Pellegrini, and M. Sala, *On the Hermitian curve and its intersections with some conics*, Tech. report, Talk at MEGA 2013, 2013.

[RS94] H. G. Ruck and H. Stichtenoth, *A characterization of Hermitian function fields over finite fields*, Journal fur die Reine und Angewandte Mathematik **457** (1994), 185–188.

[Sti88] H. Stichtenoth, *A note on Hermitian codes over GF(q^2)*, IEEE Trans. Inform. Theory **34** (1988), no. 5, 1345–1348.

[Sti93] ———, *Algebraic function fields and codes*, Universitext, Springer-Verlag, Berlin, 1993.

[Xin95] C. Xing, *On automorphism groups of the Hermitian codes*, Information Theory, IEEE Transactions on **41** (1995), no. 6, 1629–1635.