Rational points and inflexions on Hermitian-relative curves

Seon Jeong Kim

Gyeongsang National University, Korea
(joint work with Masaaki Homma)

WCC 2026
June 8-12, 2026, Paris (France)

Notations

- $\mathbb{F}_q$, the finite field with q elements, where q is a power of a prime number
- $\mathbb{P}^2$, the projective plane over the algebraic closure $\overline{\mathbb{F}}_q$ of $\mathbb{F}_q$
- $\mathbb{P}^2(\mathbb{F}_q) := \{(\alpha, \beta, \gamma) \in \mathbb{P}^2 \mid \alpha, \beta, \gamma \in \mathbb{F}_q\}$, the set of $\mathbb{F}_q$-rational points of $\mathbb{P}^2$
- For a non-constant $\mathbb{F}_q$-polynomial f in $\mathbb{F}_q[x, y, z]$, the zero set $V(f)$ of f,
  $V(f) := \{P \in \mathbb{P}^2 \mid f(P) = 0\}$, the $\mathbb{F}_q$-curve
- For an $\mathbb{F}_q$-curve $C = V(f)$,
  $C(\mathbb{F}_q) := \{(\alpha, \beta, \gamma) \in C \mid \alpha, \beta, \gamma \in \mathbb{F}_q\} = C \cap \mathbb{P}^2(\mathbb{F}_q)$, the set of $\mathbb{F}_q$-rational points of C
- $N_q(C) := |C(\mathbb{F}_q)|$, the number of $\mathbb{F}_q$-points of C

Notations

- For a point P on a curve C, $\mathcal{L}_P C$ means the tangent line to C at P.
- In this note, ω denotes a primitive element of $\mathbb{F}_q$, i.e., $\mathbb{F}_q = \{0\} \cup \{\omega^i \mid i = 0, 1, \ldots, q-2\}$.
- For $T = \begin{pmatrix} t_{11} & t_{12} & t_{13} \\ t_{21} & t_{22} & t_{23} \\ t_{31} & t_{32} & t_{33} \end{pmatrix} \in GL(3, \mathbb{F}_q)$ where q is a square,

  we denote $T^* = (T^{(\sqrt{q})})^t = \begin{pmatrix} t_{11}^{\sqrt{q}} & t_{21}^{\sqrt{q}} & t_{31}^{\sqrt{q}} \\ t_{12}^{\sqrt{q}} & t_{22}^{\sqrt{q}} & t_{32}^{\sqrt{q}} \\ t_{13}^{\sqrt{q}} & t_{23}^{\sqrt{q}} & t_{33}^{\sqrt{q}} \end{pmatrix}$.

A Hermitian curve

- Suppose that q is an even power of a prime number. (Hence $\sqrt{q}$ is an integer.)
- A Hermitian curve is the curve defined by the equation

$$x^{\sqrt{q}+1} + y^{\sqrt{q}+1} + z^{\sqrt{q}+1} = 0$$

$$\Leftrightarrow \begin{pmatrix} x^{\sqrt{q}} & y^{\sqrt{q}} & z^{\sqrt{q}} \end{pmatrix} \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix} = 0$$

$$\leftrightarrow A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

or

$$x^{\sqrt{q}+1} = y^{\sqrt{q}}z + yz^{\sqrt{q}} \quad \leftrightarrow A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & -1 \\ 0 & -1 & 0 \end{pmatrix}.$$

A Hermitian curve and its relative

- Let $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \in PGL(3, \mathbb{F}_q)$, and C_A the plane curve defined by

$$0 = \begin{pmatrix} x^{\sqrt{q}} & y^{\sqrt{q}} & z^{\sqrt{q}} \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix} \begin{pmatrix} x \\ y \\ z \end{pmatrix}$$
$$= a_{11}x^{\sqrt{q}+1} + a_{12}x^{\sqrt{q}}y + a_{13}x^{\sqrt{q}}z + a_{21}xy^{\sqrt{q}} + a_{22}y^{\sqrt{q}+1}$$
$$+ a_{23}y^{\sqrt{q}}z + a_{31}xz^{\sqrt{q}} + a_{32}yz^{\sqrt{q}} + a_{33}z^{\sqrt{q}+1}.$$

We call such a curve a Hermitian-relative curve.

Equivalence of Hermitian-relative curves

Under the coordinate transformation

$$\begin{pmatrix} x' \\ y' \\ z' \end{pmatrix} = T^{-1} \begin{pmatrix} x \\ y \\ z \end{pmatrix} \text{ with } T \in PGL(3, \mathbb{F}_q),$$

we obtain the following identity:

$$\begin{pmatrix} x^{\sqrt{q}} & y^{\sqrt{q}} & z^{\sqrt{q}} \end{pmatrix} A \begin{pmatrix} x \\ y \\ z \end{pmatrix} = \begin{pmatrix} x'^{\sqrt{q}} & y'^{\sqrt{q}} & z'^{\sqrt{q}} \end{pmatrix} T^* A T \begin{pmatrix} x' \\ y' \\ z' \end{pmatrix}.$$

Thus, two Hermitian-relative curves C_A and C_B are projectively equivalent over $\mathbb{F}_q$ if and only if there is a matrix $T \in PGL(3, \mathbb{F}_q)$ such that $B = T^* A T$ in $PGL(3, \mathbb{F}_q)$. Recall that A and B are said to be congruent in linear algebra.

In this sense, a Hermitian-relative curve C_A is a Hermitian curve if and only if $A = A^*$.

Pardini's Theorem

Theorem 1 (Pardini, 1986).

Let $f(x,y,z) \in \mathbb{F}_q[x,y,z]$ be a homogeneous polynomial of degree $\sqrt{q}+1$. The curve C defined by $f(x,y,z)=0$ in $\mathbb{P}^2$ is projectively equivalent over $\overline{\mathbb{F}}_q$ to a Hermitian curve of degree $\sqrt{q}+1$ if and only if C is a Hermitian-relative curve, that is, there exists $A \in PGL(3,\mathbb{F}_q)$ such that

$$f(x,y,z) = \begin{pmatrix} x^{\sqrt{q}} & y^{\sqrt{q}} & z^{\sqrt{q}} \end{pmatrix} A \begin{pmatrix} x \\ y \\ z \end{pmatrix}.$$

Number of $\mathbb{F}_q$-points of a Hermitian-relative curve

Recall that $N_q(C_A) = |C_A(\mathbb{F}_q)|$ is the number of $\mathbb{F}_q$-points of C_A.

Theorem 2 (Homma-K, 2024).

$N_q(C_A) \equiv 1 \pmod{\sqrt{q}}$. *In particular, $C_A(\mathbb{F}_q)$ is not empty.*

- (well known) If C_A is Hermitian, then $N_q(C_A) = \sqrt{q}^3 + 1$.
- For any $P \in C_A$, $i(C_A \bullet \mathcal{L}_P(C_A); P) = \sqrt{q}$ or $\sqrt{q} + 1$. A point P is called an inflexion if $i(C_A \bullet \mathcal{L}_P(C_A); P) = \sqrt{q} + 1$.
- If C_A is Hermitian, all points of $C_A(\mathbb{F}_q)$ are inflexions.
- Denote $I_q(C)$ the number of rational inflexions on C. We say that a curve C is of type (n, i) if $N_q(C) = n$ and $I_q(C) = i$.

The mirror of C_A

Proposition 1 (Homma-K, 2024).

- *C_{A^*} is called the mirror of C_A;*
  C_A is Hermitian $\Leftrightarrow$ $C_A = C_{A^*}$.
- $C_A(\mathbb{F}_q) = C_{A^*}(\mathbb{F}_q)$
- *Let P be an $\mathbb{F}_q$-point. Then P is an inflexion of C_A $\Leftrightarrow$ P is an inflexion of C_{A^*}.*
  In this case, $i(C_A \bullet C_{A^*}; P) \geq \sqrt{q} + 1$ if C_A (or C_{A^*}) is not Hermitian.

- If C_A is not Hermitian, then $N_q(C_A) \leq (\sqrt{q} + 1)^2$, and if equality holds, then C_A has no (rational) inflexions.

A bijection φ_A between $\mathbb{F}_q$-points

Proposition 2.

Let $A \in PGL(3,q)$ be a nonsingular matrix over a field $\mathbb{F}_q$, and C_A the Hermitian-relative curve corresponding to A. Let $\varphi_A : C_A(\overline{\mathbb{F}}_q) \to C_A(\overline{\mathbb{F}}_q)$ be a map defined by $\varphi_A(P) = Q$, where $P \in C_A(\overline{\mathbb{F}}_q)$ and $C \bullet \mathcal{L}_P C_A = \sqrt{q}\, P + Q$. Then, for $P = (x_0, y_0, z_0)$, we have

$$\varphi_A(P) = \varphi_A(x_0, y_0, z_0) = (A^{-1} A^* (x_0^q, y_0^q, z_0^q)^t)^t.$$

Classification of the C_A's with at least two $\mathbb{F}_q$-inflexions

Let C be a Hermitian-relative curve with at least two rational inflexions. We may choose a system of coordinates of $\mathbb{P}^2$ over $\mathbb{F}_q$ such that

- $P = (1, 0, 0)$ and $Q = (0, 1, 0)$ are inflexions of C
- $\mathcal{L}_P(C) = \{y = 0\}$ and $\mathcal{L}_Q(C) = \{x = 0\}$.

A direct calculation shows that curve C is projejctively equivalent to the following curve.

$$x^{\sqrt{q}}y + \eta x y^{\sqrt{q}} + z^{\sqrt{q}+1} = 0, \quad A = \begin{pmatrix} 0 & 1 & 0 \\ \eta & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

Classification of the C_A's with at least two $\mathbb{F}_q$-inflexions

Depending on the value of the coefficient η in the above equation, we have the following results. (Homma-K, 2024)

	$N_q(C_A)$	$I_q(C_A)$	classes
$\eta = 1$	$\sqrt{q}^3 + 1$	$\sqrt{q}^3 + 1$	1 (Hermitian)
$Nm\,\eta = 1$ and $\eta \neq 1$	$\sqrt{q} + 1$	$\sqrt{q} + 1$	$\sqrt{q}$
$Nm\,\eta \neq 1$	$q + 1$	2	$\frac{1}{2}(\sqrt{q} + 1)(\sqrt{q} - 2)$

Here $Nm : \mathbb{F}_q^* \to \mathbb{F}_{\sqrt{q}}^*$ is the norm defined by $Nm(x) = x^{\sqrt{q}+1}$.

To find the number of classes, we use the following:

$$\begin{pmatrix} 0 & 1 & 0 \\ \eta & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \sim \begin{pmatrix} 0 & 1 & 0 \\ \eta' & 0 & 0 \\ 0 & 0 & 1 \end{pmatrix} \Leftrightarrow \eta' = \eta \text{ or } \eta^{-\sqrt{q}}.$$

A Classification of the C_A's from another viewpoint

Table: Classification

	Case A: **All Rational Points are Inflections**	**Case B:** **Has Non-inflection Rational Points**
Case 1: $\geq$ 2 **Inflections**	Classified	Classified
Case 2: $\leq$ 1 **Inflection**	Remaining	Remaining

A HR curve with only one $\mathbb{F}_q$-point

We classify Hermitian-relative curves with only one $\mathbb{F}_q$-point. Then such curves satisfy the condition that all $\mathbb{F}_q$-points are inflexions. Let C be such a curve with only one $\mathbb{F}_q$-point P. We may choose a system of coordinates of $\mathbb{P}^2$ over $\mathbb{F}_q$ such that

- $P = (1, 0, 0)$ is an inflexion of C
- $\mathcal{L}_P(C) = \{y = 0\}$.

A direct calculation shows that curve C is projejctively equivalent to the following curve.

Theorem 3.

$x^{\sqrt{q}+1} + \eta y^{\sqrt{q}+1} + y^{\sqrt{q}} z + y z^{\sqrt{q}} = 0$ with $\eta \in \mathbb{F}_q \setminus \mathbb{F}_{\sqrt{q}}$. Furthermore, two curves arising from $\eta, \eta' \in \mathbb{F}_q \setminus \mathbb{F}_{\sqrt{q}}$ are projectively equivalent over $\mathbb{F}_q$.

Theorem 4.

There exist Hermitian-relative curves of types $(q\sqrt{q}+1, q\sqrt{q}+1)$, $(\sqrt{q}+1, \sqrt{q}+1)$, and $(1,1)$. Moreover, if $N_q(C) = I_q(C)$ for a Hermitian-relative curve C, then its type must be one of these three cases.

- $N_q(C) = q\sqrt{q}+1$ if and only if C is a Hermition curve.
- $N_q(C) = \sqrt{q}+1$ if and only if C is projectively equivalent to the curve $x^{\sqrt{q}+1} + y^{\sqrt{q}+1} + \eta z^{\sqrt{q}+1} = 0$ with $\eta \in \mathbb{F}_q \setminus \mathbb{F}_{\sqrt{q}}$.
- $N_q(C) = 1$ if and only if C is projectively equivalent to the curve $x^{\sqrt{q}+1} + \eta y^{\sqrt{q}+1} + y^{\sqrt{q}}z + yz^{\sqrt{q}} = 0$ with $\eta \in \mathbb{F}_q \setminus \mathbb{F}_{\sqrt{q}}$.

The corresponding matrices are as follows;

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & \eta \end{pmatrix}, \begin{pmatrix} 1 & 0 & 0 \\ 0 & \eta & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Curves with $N_q(C) > I_q(C)$

Let C be a Hermitian-relative curve wiht an $\mathbb{F}_q$-point P which is not an inflexion. We may choose a system of coordinates of $\mathbb{P}^2$ over $\mathbb{F}_q$ such that

- $P = (1, 0, 0)$, $\varphi(P) = (0, 1, 0)$, and $\varphi^2(P) = (0, 0, 1)$.
- $\mathcal{L}_P C = \{z = 0\}$ and $T_{\varphi(P)} C = \{x = 0\}$.

A direct calculation shows that curve C is projejctively equivalent to the following curve.

Theorem 5.

If a Hermitian-relative curve C has an $\mathbb{F}_q$-point which is not an inflexion, then it is projectively equivalent to

$$C_{a,b} : \ x^{\sqrt{q}}z + xy^{\sqrt{q}} + bx^{\sqrt{q}}z + ayz^{\sqrt{q}} = 0$$

where $a, b \in \mathbb{F}_q$, $a \neq 0$.

Classification of curves $C_{a,b}$ with $b = 0$

Theorem 6.

For a Hermitian-relative curve

$$C_{a,0}: \; x^{\sqrt{q}}z + xy^{\sqrt{q}} + ayz^{\sqrt{q}} = 0,$$

the following hold:

- *If* $\sqrt{q} \equiv 0 \pmod 3$, *then* $C_{a,0}$ *is of type* $(q+1, 1)$.
- *If* $\sqrt{q} \equiv 1 \pmod 3$, *then* $C_{a,0}$ *is of type* $(q+1, 2)$.
- *If* $\sqrt{q} \equiv 2 \pmod 3$, *then* $C_{a,0}$ *is of type* $(q + 2\sqrt{q} + 1, 0)$ *for* $a = \omega^{3j}$, $0 \le j < \frac{q-1}{3}$ *and* $(q - \sqrt{q} + 1, 0)$, *otherwise. Here* ω *is a primitive element of* $\mathbb{F}_q$.

Transform $C_{a,b}$ $(a, b \in \mathbb{F}_q^*)$ into a simpler form

The curve $C_{a,b}$: $x^{\sqrt{q}}z + xy^{\sqrt{q}} + bx^{\sqrt{q}}z + ayz^{\sqrt{q}} = 0$, $a, b \in \mathbb{F}_q^*$ is corresponds to the matrix $A_{a,b} = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ b & a & 0 \end{pmatrix}$. If we let $T = \begin{pmatrix} ba^{\sqrt{q}} & 0 & 0 \\ 0 & -b^{\sqrt{q}} & 0 \\ 0 & 0 & 1 \end{pmatrix}$, then $T^* A_{a,b} T = \begin{pmatrix} 0 & 0 & 1 \\ -c & 0 & 0 \\ c & -1 & 0 \end{pmatrix}$ in $PGL(3, \mathbb{F}_q)$, where $c = b(\frac{a}{b})^{\sqrt{q}-1}$.

Theorem 7.

The Hermitian-relative curve $C_{a,b}$, $(a, b \in \mathbb{F}_q^*)$ is projectively equivalent to C_c, $c \in \mathbb{F}_q^*$, where

$$C_c : \ x^{\sqrt{q}}z - cxy^{\sqrt{q}} + cxz^{\sqrt{q}} - yz^{\sqrt{q}} = 0.$$

Furthermore, any C_c, $c \in \mathbb{F}_q^*$, is projectively equivalent to $C_{a,b}$ for some $a, b \in \mathbb{F}_q^*$.

The intersection of a line $y = y_0$ and C_c

We want to find the numbers of rational points and inflexions of the curve

$$C_A : \ x^{\sqrt{q}}z - cxy^{\sqrt{q}} + cxz^{\sqrt{q}} - yz^{\sqrt{q}} = 0. \ \leftrightarrow \ A = \begin{pmatrix} 0 & 0 & 1 \\ -c & 0 & 0 \\ c & -1 & 0 \end{pmatrix}$$

We have the following:

- $\{z = 0\} \cap C_A(\mathbb{F}_q) = \{(1,0,0),(0,1,0)\}$.
- $\left|\{y = y_0\} \cap C_A^{\circ}\right| = 1$ if $Nm(c(y_0^{\sqrt{q}} - 1)) \neq 1$, where $C_A^{\circ} : \ x^{\sqrt{q}} - cxy^{\sqrt{q}} + cx - y = 0$ is the affine part of C_A, i.e., $C_A \cap \{z \neq 0\}$.
- $\left|\{y = y_0\} \cap C_A^{\circ}\right| = \sqrt{q}$ if $Nm(c(y_0^{\sqrt{q}} - 1)) = 1$ and $y^{\sqrt{q}-1} + c^{\sqrt{q}}y - c^{\sqrt{q}} = 0$.
- $\left|\{y = y_0\} \cap C_A^{\circ}\right| = 0$ if $Nm(c(y_0^{\sqrt{q}} - 1)) = 1$ and $y^{\sqrt{q}-1} + c^{\sqrt{q}}y - c^{\sqrt{q}} \neq 0$.

The number of rational points of C_c

Since $\left|\{y_0 \in \mathbb{F}_q \mid Nm(c(y_0^{\sqrt{q}} - 1)) \neq 1\}\right| = q - (\sqrt{q} + 1)$, and

$$\begin{aligned}
C_A(\mathbb{F}_q) &= \{(1,0,0),(0,1,0)\} \cup C_A^\circ(\mathbb{F}_q) \\
&= \{(1,0,0),(0,1,0)\} \cup \bigcup_{y_0 \in \mathbb{F}_q} (\{y = y_0\} \cap C_A^\circ(\mathbb{F}_q)) \\
&= \{(1,0,0),(0,1,0)\} \cup \bigcup_{Nm(c(y_0^{\sqrt{q}}-1)) \neq 1} (\{y = y_0\} \cap C_A^\circ(\mathbb{F}_q)) \\
&\cup \{(1,0,0),(0,1,0)\} \cup \bigcup_{Nm(c(y_0^{\sqrt{q}}-1)) = 1} (\{y = y_0\} \cap C_A^\circ(\mathbb{F}_q)),
\end{aligned}$$

we have $|C_A(\mathbb{F}_q)| = q - \sqrt{q} + 1 + s\sqrt{q}$, where $s = \left|\{y_0 \in \mathbb{F}_q \mid Nm(c(y_0^{\sqrt{q}} - 1)) = 1 \text{ and } y_0^{\sqrt{q}-1} + c^{\sqrt{q}} y - c^{\sqrt{q}} = 0\}\right|$.
Thus it is obvious that $|C_A(\mathbb{F}_q)| \geq q - \sqrt{q} + 1$.

Eigenvalues and eigenvectors of $U = A^{-1}A^*$

Let $U = A^{-1}A^*$. Recall that, for $P = (x_0, y_0, z_0)^t \in C_A(\mathbb{F}_q)$

- $\varphi_A(P) = (A^{-1}A^*)P = UP$. (by Proposition 2)
- $\mathcal{L}_P C_\bullet C_A = \sqrt{q}P + \varphi_A(P)$.
- P is an inflexion of $C_A \Leftrightarrow \varphi_A(P) = P$.

The characteristic polynomial of U is

$$P_U(\lambda) = \lambda^3 - c^{\sqrt{q}}\lambda^2 + c^{\sqrt{q}}\lambda - c^{\sqrt{q}-1}.$$

If $P_U(\lambda_0) = 0$, then the corresponding eigenvector is $(\frac{1}{c\lambda_0}, 1 - c^{-\sqrt{q}}\lambda_0, 1)$.

Lemma 8.

Two matrices U^* and U^{-1} are similar to each other. So we have $P_{U^*}(\lambda) = P_{U^{-1}}(\lambda)$. Therefore, if λ_0 is an eigenvalue of U, then $\lambda_0^{\sqrt{q}} = \lambda_1^{-1}$ for some eigenvalue λ_1 of U. Note that λ_0 need not be equal to λ_1.

Classification of characteristic polynomials $P_U(\lambda)$

Proposition 3.

The polynomial $P_U(\lambda)$ satisfies one of the following:

(i) *$P_U(\lambda)$ has the triple root. In this case, the triple root is 1 and it occurs only when $c = 3$ and $p \neq 3$.*

(ii) *$P_U(\lambda)$ has one double root and the other simple root. In this case, both roots belong to $\mu_{\sqrt{q}+1}$.*

(iii) *$P_U(\lambda)$ has three simple roots, all of which belong to $\mu_{\sqrt{q}+1}$.*

(iv) *$P_U(\lambda)$ has three simple roots, only one of which belongs to $\mu_{\sqrt{q}+1}$, and the other two, say β and γ satisfy $\beta^{\sqrt{q}} = \gamma^{-1}$.*

(v) *$P_U(\lambda)$ is irreducible.*

Remark. $P_U(\lambda)$ can not have an irreducible factor of degree 2.

Eigenvalues, eigenvectors, inflexions and $\sqrt{q}$-lines

Denote $\mu_{\sqrt{q}+1} = \{\zeta \in \mathbb{F}_q \mid \zeta^{\sqrt{q}+1} = 1\}$ the set of $(\sqrt{q}+1)$-th root of unity. We have the following:

- If λ_0 is a root of $P_U(\lambda)$, i.e., an eigenvalue of U, then $(\frac{1}{c\lambda_0}, 1 - c^{-\sqrt{q}}\lambda_0, 1)$ is an inflexion or $y = 1 - c^{-\sqrt{q}}\lambda_0$ is a $\sqrt{q}$-line of C_A°, which means $\left|\{y = 1 - c^{-\sqrt{q}}\lambda_0\} \cap C_A^\circ\right| = \sqrt{q}$.
- If λ_0 is a double or triple root of $P_U(\lambda)$, then $\lambda_0 \in \mu_{\sqrt{q}+1}$ and $(\frac{1}{c\lambda_0}, 1 - c^{-\sqrt{q}}\lambda_0, 1)$ is an inflexion, and $y = 1 - c^{-\sqrt{q}}\lambda_0$ is a $\sqrt{q}$-line of C_A°.
- If $\lambda_0 \in \mu_{\sqrt{q}+1}$ is a root of $P_U(\lambda)$, then $y = 1 - c^{-\sqrt{q}}\lambda_0$ is a $\sqrt{q}$-line of C_A°.
- If $\lambda_0 \notin \mu_{\sqrt{q}+1}$ is a root of $P_U(\lambda)$, then $(\frac{1}{c\lambda_0}, 1 - c^{-\sqrt{q}}\lambda_0, 1)$ is an inflexion.
- If $(x_0, y_0, 1)$ is an inflexion, then $\lambda_0 = c^{\sqrt{q}}(1 - y_0)$ is a root of $P_U(\lambda)$, i.e., an eigenvalue of U.
- If $y = y_0$ ia a $\sqrt{q}$-line of C_A°, then $\lambda_0 = c^{\sqrt{q}}(1 - y_0)$ is a root of $P_U(\lambda)$, i.e., an eigenvalue of U.

- If $P_U(\lambda)$ has three distinct roots α_i, $i = 1, 2, 3$, which belong to $\mu_{\sqrt{q}+1}$, then the three corresponding lines $y = 1 - c^{-\sqrt{q}}\alpha_i$ are all $\sqrt{q}$-lines of C_c° and C_c has no inflexion.
- Suppose that $P_U(\lambda)$ has three distinct roots, exactly one of which belongs to $\mu_{\sqrt{q}+1}$. Then the two eigenvectors corresponding to the other two eigenvalues are inflexions of C_c.

Consider the set of polynomials $\mathcal{P} = \{f_c \mid c \in \mathbb{F}_q^*\}$, where $f_c(\lambda) = \lambda^3 - c^{\sqrt{q}}\lambda^2 + c^{\sqrt{q}}\lambda - c^{\sqrt{q}-1}$.

- If $\alpha, \beta, \gamma \in \mu_{\sqrt{q}+1}$ and $\alpha + \beta + \gamma = \alpha\beta + \beta\gamma + \alpha\gamma \neq 0$, then α, β, and γ are the roots of the polynomial f_c, where $c = (\alpha + \beta + \gamma)^{\sqrt{q}}$.
- For $p \neq 2, 3$ and $\alpha \in \mu_{\sqrt{q}+1}$, there exists an element $c \in \mathbb{F}_q^*$ such that α is a double root of the polynomial f_c. Moreover, the remaining root of f_c is given by $\frac{\alpha(2-\alpha)}{2\alpha-1}$, which also belongs to $\mu_{\sqrt{q}+1}$.

Eigenvalues, eigenvectors, inflexions and $\sqrt{q}$-lines

- For the cases $p = 2$ and $p = 3$, the following statements hold.
  - When $p = 2$, for each $\alpha \in \mu_{\sqrt{q}+1}$, the polynomial f_c, $c = \alpha^{2\sqrt{q}}$, has α as a double root and the other root is α^2.
  - When $p = 3$, if the polynomial f_c (with $c \neq 0$) possesses a double root α, then it must be $\alpha = 2$. Specifically, for $\alpha = 2 \in \mu_{\sqrt{q}+1}$ and any $\beta \in \mu_{\sqrt{q}+1} \setminus \{2\}$, the polynomial f_c with $c = (1+\beta)^{\sqrt{q}}$ has 2 as a double root and β as the remaining simple root.
- Suppose that $\alpha, \beta \in \mu_{\sqrt{q}+1}$ are roots of f_c for some $c \in \mathbb{F}_q^*$.
  - If $\alpha + \beta \neq 1$ and $\alpha^2 + \alpha\beta + \beta^2 \neq 0$, then the third root γ belongs to $\mu_{\sqrt{q}+1}$, and γ and c are explicitly given by

$$\gamma = \frac{\alpha+\beta-\alpha\beta}{\alpha+\beta-1} \quad \text{and} \quad c = \left(\frac{\alpha^2+\alpha\beta+\beta^2}{\alpha+\beta-1}\right)^{\sqrt{q}}.$$

  - If $\alpha + \beta = 1$, then it necessarily follows that $\alpha\beta = 1$. Furthermore, for any $\gamma \in \mu_{\sqrt{q}+1} \setminus \{-1\}$, the elements α, β, γ are the roots of $f_c(\lambda)$ with $c = (1+\gamma)^{\sqrt{q}} = 1 + \gamma^{\sqrt{q}}$.

Classification of HR curves C_c with $c \in \mathbb{F}_q^*$

- The solutions to the system of equations $\begin{cases} \alpha\beta = 1 \\ \alpha + \beta = 1 \end{cases}$ over $\mathbb{F}_q$ are given as follows:
  - If q is even (i.e., $p = 2$), then $\{\alpha, \beta\} = \left\{\omega^{\frac{q-1}{3}}, \omega^{\frac{2(q-1)}{3}}\right\}$.
  - If $3 \mid q$ (i.e., $p = 3$), then $\alpha = \beta = -1 = 2$.
  - If $p \neq 2, 3$, then $\{\alpha, \beta\} = \left\{\omega^{\frac{q-1}{6}}, \omega^{\frac{5(q-1)}{6}}\right\}$.
- Let $\alpha \in \mu_{\sqrt{q}+1}$ and $\beta, \gamma \in \mathbb{F}_q$ satisfying $\gamma = \beta^{-\sqrt{q}}$. If $\alpha + \beta + \gamma = \alpha\beta + \beta\gamma + \gamma\alpha \neq 0$, then α, β, γ are the roots of the polynomial $f_c(\lambda)$, where $c = (\alpha + \beta + \gamma)^{\sqrt{q}}$.
- Let β and γ be elements of $\mathbb{F}_q$ such that $\beta^{\sqrt{q}} = \gamma^{-1}$
  - If $\beta + \gamma \neq 1$ and $\beta^2 + \beta\gamma + \gamma^2 \neq 0$, let $\alpha = \frac{\beta+\gamma-\beta\gamma}{\beta+\gamma-1}$. Then $\alpha \in \mu_{\sqrt{q}+1}$ and α, β, γ are the roots of f_c for $c = \left(\frac{\beta^2+\beta\gamma+\gamma^2}{\beta+\gamma-1}\right)^{\sqrt{q}}$.
  - If $\beta + \gamma = 1$, then $\gamma = \beta^{-1} \in \mathbb{F}_{\sqrt{q}}$ and $c^{\sqrt{q}-1}, \beta, \gamma$ are the roots of f_c, where c satisfies the relation $c^{\sqrt{q}} - c^{\sqrt{q}-1} - 1 = 0$.

Classification of HR curves C_c with $c \in \mathbb{F}_q^*$

- Let α and β be $(\sqrt{q}+1)$-th roots of unity in $\mathbb{F}_q$. Suppose that $\alpha + \beta = 1$. Then $\alpha\beta = 1$ and the following statements hold:
  - The case $q \equiv 0 \pmod 2$ (Characteristic $p = 2$): If $\sqrt{q} \equiv 2 \pmod 3$, then the solutions are:

    $$\begin{cases} \alpha = \omega^{\frac{q-1}{3}} \\ \beta = \alpha^{-1} = \omega^{\frac{2(q-1)}{3}} \end{cases} \quad \text{or} \quad \begin{cases} \alpha = \omega^{\frac{2(q-1)}{3}} \\ \beta = \alpha^{-1} = \omega^{\frac{q-1}{3}} \end{cases}$$

    If $\sqrt{q} \equiv 1 \pmod 3$, then there is no solution.
  - The case $q \equiv 0 \pmod 3$ (Characteristic $p = 3$): The only solution is $\alpha = \beta = 2$.
  - The other cases ($p \neq 2, 3$): If $\sqrt{q} \equiv 2 \pmod 3$, then the solutions are:

    $$\begin{cases} \alpha = \omega^{\frac{q-1}{6}} \\ \beta = \alpha^{-1} = \omega^{\frac{5(q-1)}{6}} \end{cases} \quad \text{or} \quad \begin{cases} \alpha = \omega^{\frac{5(q-1)}{6}} \\ \beta = \alpha^{-1} = \omega^{\frac{q-1}{6}} \end{cases}$$

    If $\sqrt{q} \equiv 1 \pmod 3$, then there is no solution.

Classification of HR curves C_c with $c \in \mathbb{F}_q^*$

- Let α and β be elements of $\mathbb{F}_q$ such that $\alpha^{\sqrt{q}} = \beta^{-1}$ and $\alpha + \beta = 1$. Then the following statements hold:
  - Case $q \equiv 0 \pmod 2$: If $\sqrt{q} \equiv 1 \pmod 3$, the solutions are:

$$\begin{cases} \alpha = \omega^{\frac{q-1}{3}} \\ \beta = \alpha^{-1} = \omega^{\frac{2(q-1)}{3}} \end{cases} \quad \text{or} \quad \begin{cases} \alpha = \omega^{\frac{2(q-1)}{3}} \\ \beta = \alpha^{-1} = \omega^{\frac{q-1}{3}} \end{cases}$$

    If $\sqrt{q} \equiv 2 \pmod 3$, there is no solution.
  - Case $q \equiv 0 \pmod 3$: The unique solution is $\alpha = \beta = 2$, which belongs to the group of $(\sqrt{q}+1)$-th roots of unity, $\mu_{\sqrt{q}+1}$.
  - Case $p \neq 2, 3$: If $\sqrt{q} \equiv 1 \pmod 3$, the solutions are:

$$\begin{cases} \alpha = \omega^{\frac{q-1}{6}} \\ \beta = \alpha^{-1} = \omega^{\frac{5(q-1)}{6}} \end{cases} \quad \text{or} \quad \begin{cases} \alpha = \omega^{\frac{5(q-1)}{6}} \\ \beta = \alpha^{-1} = \omega^{\frac{q-1}{6}} \end{cases}$$

    If $\sqrt{q} \equiv 2 \pmod 3$, there is no solution.

Classification of HR curves C_c with $c \in \mathbb{F}_q^*$

- Consider the equation $\alpha^2 + \alpha\beta + \beta^2 = 0$ for $\alpha, \beta \in \mu_{\sqrt{q}+1}$.
  - Case $\sqrt{q} \equiv 0 \pmod 3$: The equation is satisfied if and only if $\alpha = \beta$.
  - Case $\sqrt{q} \equiv 1 \pmod 3$: The equation has no solutions in $\mu_{\sqrt{q}+1}$.
  - Case $\sqrt{q} \equiv 2 \pmod 3$: The solutions are $\beta = \alpha\omega^{\frac{q-1}{3}}$ and $\beta = \alpha\omega^{\frac{2(q-1)}{3}}$.
- Consider the equation $\alpha^2 + \alpha\beta + \beta^2 = 0$ for $\alpha, \beta \in \mathbb{F}_q$ such that $\alpha^{\sqrt{q}} = \beta^{-1}$. Then the following statements hold:
  - Case $\sqrt{q} \equiv 0 \pmod 3$: The equation is satisfied if and only if $\alpha = \beta$. In this case, α (and thus β) necessarily belongs to $\mu_{\sqrt{q}+1}$.
  - Case $\sqrt{q} \equiv 1 \pmod 3$: The solutions are given by $\beta = \alpha\omega^{\frac{q-1}{3}}$ or $\beta = \alpha\omega^{\frac{2(q-1)}{3}}$.
  - Case $\sqrt{q} \equiv 2 \pmod 3$: There are no solutions satisfying the given conditions.

Classification of HR curves C_c with $c \in \mathbb{F}_q^*$

- Let three sets S_1, S_2 and S_3 as follows;

$$S_1 = \{(\alpha,\beta,\gamma) \in (\mu_{\sqrt{q}+1})^3 \mid \alpha,\beta,\gamma \text{ are roots of } f_c \text{ for some } c \in \mathbb{F}_q^*\}$$

$$S_2 = \{(\alpha,\beta,\gamma) \in (\mu_{\sqrt{q}+1})^3 \mid \alpha+\beta \neq 1,\ \alpha^2+\alpha\beta+\beta^2 \neq 0,\ \gamma = \frac{\alpha+\beta-\alpha\beta}{\alpha+\beta-1}\}$$

$$S_3 = \{(\alpha,\beta,\gamma) \in (\mu_{\sqrt{q}+1})^3 \mid \alpha+\beta = 1,\ \gamma \neq -1\}.$$

  Then S_1 is the disjoint union of S_2 and S_3.

- For $\sqrt{q} \equiv 0 \pmod 3$, we observe the following properties.
  - There exists no polynomial f_c with $c \neq 0$ that possesses a triple root.
  - The number of polynomials f_c having a double root is $\sqrt{q}$. In this case, both the double root and the remaining simple root belong to $\mu_{\sqrt{q}+1}$.
  - The number of polynomials f_c that have three distinct roots, all of which belong to $\mu_{\sqrt{q}+1}$,

    is given by $\dfrac{q-\sqrt{q}}{6}$.

Classification of HR curves C_c with $c \in \mathbb{F}_q^*$

- For $\sqrt{q} \equiv 1 \pmod 3$, we observe the following properties.
  - There exists a unique polynomial f_c with $c \neq 0$ that has a triple root. In this case, the triple root is 1 and $c = 3$ (or $c = 1$ if $p = 2$).
  - The number of polynomials f_c having a double root is $\sqrt{q}$. In this case, both the double root and the remaining simple root belong to $\mu_{\sqrt{q}+1}$.
  - The number of polynomials f_c that have three distinct roots, all of which belong to $\mu_{\sqrt{q}+1}$, is given by $\dfrac{q-\sqrt{q}}{6}$.
- For $\sqrt{q} \equiv 2 \pmod 3$, we observe the following properties.
  - There exists a unique polynomial f_c with $c \neq 0$ that has a triple root. In this case, the triple root is 1 and $c = 3$ (or $c = 1$ if $p = 2$).
  - The number of polynomials f_c having a double root is $\sqrt{q}$. In this case, both the double root and the remaining simple root belong to $\mu_{\sqrt{q}+1}$.
  - The number of polynomials f_c that have three distinct roots, all of which belong to $\mu_{\sqrt{q}+1}$, is given by $\dfrac{q-\sqrt{q}-2}{6}$.

Classification of HR curves C_c with $c \in \mathbb{F}_q^*$

- The number of characteristic polynomials that have three distinct simple roots, where only one of them belongs to $\mu_{\sqrt{q}+1}$, is:

$$\begin{cases} \dfrac{q-\sqrt{q}-2}{2} & \text{when } \sqrt{q} \equiv 0 \pmod 3 \\ \dfrac{q-\sqrt{q}-4}{2} & \text{when } \sqrt{q} \equiv 1 \pmod 3 \\ \dfrac{q-\sqrt{q}-2}{2} & \text{when } \sqrt{q} \equiv 2 \pmod 3 \end{cases}$$

- The number of irreducible characteristic polynomials f_c, $c \in \mathbb{F}_q^*$ over $\mathbb{F}_q$ is:

$$\begin{cases} \dfrac{q-\sqrt{q}}{3} & \text{when } \sqrt{q} \equiv 0 \pmod 3 \\ \dfrac{q-\sqrt{q}}{3} & \text{when } \sqrt{q} \equiv 1 \pmod 3 \\ \dfrac{q-\sqrt{q}-2}{3} & \text{when } \sqrt{q} \equiv 2 \pmod 3 \end{cases}$$

Theorem 9.

Case	*type* (n, i)	*the number of polynomials*		
		$\sqrt{q} \equiv 0 \pmod 3$	$\sqrt{q} \equiv 1 \pmod 3$	$\sqrt{q} \equiv 2 \pmod 3$
(I)	$(q - \sqrt{q} + 1, 0)$	$\frac{q-\sqrt{q}}{3}$	$\frac{q-\sqrt{q}}{3}$	$\frac{q-\sqrt{q}-2}{3}$
(II)	$(q + 1, 1)$	*0*	*1*	*1*
(III)	$(q + 1, 2)$	$\frac{q-\sqrt{q}-2}{2}$	$\frac{q-\sqrt{q}-4}{2}$	$\frac{q-\sqrt{q}-2}{2}$
(IV)	$(q + \sqrt{q} + 1, 1)$	$\sqrt{q}$	$\sqrt{q}$	$\sqrt{q}$
(V)	$(q + 2\sqrt{q} + 1, 0)$	$\frac{q-\sqrt{q}}{6}$	$\frac{q-\sqrt{q}}{6}$	$\frac{q-\sqrt{q}-2}{6}$

In the table, “Cases” mean as follows;

(I) *f_c is an irreducible polynomial.*

(II) *f_c has a triple root.*

(III) *f_c has three simple roots, only one of them is $(\sqrt{q} + 1)$-th root of unity.*

(IV) *f_c has a double root and the other simple root, both of them are $(\sqrt{q} + 1)$-th roots of unity.*

(V) *f_c has three simple roots which are all $(\sqrt{q} + 1)$-th roots of unity.*

Classification of all Hermitian-relative curves

Using Theorems 4, 6 and 9, we obtain

Theorem 10.

Let $q > 4$. A pair (n, i) is the type of a Hermitian-relative curve if and only if (n, i) belongs to the set

$$\{(q\sqrt{q}+1, q\sqrt{q}+1), (\sqrt{q}+1, \sqrt{q}+1), (1, 1),$$
$$(q-\sqrt{q}+1, 0), (q+1, 1), (q+1, 2),$$
$$(q+\sqrt{q}+1, 1), (q+2\sqrt{q}+1, 0)\}.$$

Remark. Consider the case $q = 4$. As we see in the next table, all types except $(q+1, 2) = (5, 2)$ occur in some Hermitian-relative curve. In the case $q > 4$, the type $(q+1, 2)$ occurs when the $P_U(\lambda)$ has a root which does not belong to $\mu_{\sqrt{q}+1}$. However, for $q = 4$, every nonzero element belongs to $\mu_{\sqrt{q}+1} = \mu_3$.

The case $q = 4$, after Hirschfeld

J. W. P. Hirschfeld, Projective geometries over finite fields (second edition), Oxford University Press, Oxford, 1998 §11

$\mathbb{F}_4 = \{0, 1, \omega, \omega^2\}$, $\omega^3 = 1$

Equation of C	$N_q(C)$	$I_q(C)$	
$x^2y + xy^2 + z^3$	9	9	Hermitian
$x^2y + \omega xy^2 + z^3$	3	3	$Nm\,\omega = 1, \omega \neq 1$
$x^2y + \omega^2 xy^2 + z^3$	3	3	$Nm\,\omega^2 = 1, \omega^2 \neq 1$
$x^3 + \omega y^3 + y^2z + yz^2$	1	1	Theorem 3
$\omega x^3 + \omega y^3 + y^2z + yz^2$	7	1	$7 = q + \sqrt{q} + 1$
$\omega^2 x^3 + \omega^2 y^3 + y^2z + yz^2$	7	1	
$x^3 + xy^2 + y^2z + yz^3$	5	1	$5 = q + 1$
$x^3 + \omega y^3 + \omega^2 z^3$	9	0	$9 = (\sqrt{q} + 1)^2$
$x^2z + xy^2 + \omega yz^2$	3	0	$3 = q - \sqrt{q} + 1$
$x^2z + xy^2 + \omega^2 yz^2$	3	0	

References

- J. W. P. Hirschfeld, Projective geometries over finite fields (second edition), Oxford University Press, Oxford, 1998.
- M. Homma and S. J. Kim, Relatives of the Hermitian curve, Journal of Geometry (2026) 117:11. https://doi.org/10.1007/s00022-026-00795-8
- R. Pardini, Some remarks on plane curves over fields of finite characteristic, *Compositio Math.* **60**(1986), 3–17.

Projectively equivalence classes of all types

In WAIFI2026, Santander, Spain, we obtained the table:

Table: Classification of projective equivalence classes for each type

Type of Curve (n, i)	The number of equivalence classes		
	$\sqrt{q} \equiv 0 \pmod 3$	$\sqrt{q} \equiv 1 \pmod 3$	$\sqrt{q} \equiv 2 \pmod 3$
$(q\sqrt{q}+1, q\sqrt{q}+1)$	1	1	1
$(\sqrt{q}+1, \sqrt{q}+1)$	$\sqrt{q}$	$\sqrt{q}$	$\sqrt{q}$
$(1, 1)$	1	1	1
$(q-\sqrt{q}+1, 0)$	$\frac{q-\sqrt{q}}{3}$	$\frac{q-\sqrt{q}}{3}$	$\frac{q-\sqrt{q}+4}{3}$
$(q+1, 1)$	1	1	1
$(q+1, 2)$	$\frac{q-\sqrt{q}-2}{2}$	$\frac{q-\sqrt{q}-2}{2}$	$\frac{q-\sqrt{q}-2}{2}$
$(q+\sqrt{q}+1, 1)$	$\sqrt{q}$	$\sqrt{q}$	$\sqrt{q}$
$(q+2\sqrt{q}+1, 0)$	$\frac{q-\sqrt{q}}{6}$	$\frac{q-\sqrt{q}}{6}$	$\frac{q-\sqrt{q}+4}{6}$

Thank you for your attention!!!