On some Galois subcovers of the Hermitian curve

Arianna Dionigi

Joint work with Barbara Gatti

Università degli Studi di Perugia (Italy)

5th Pythagorean conference
June 1-6, 2025 - Kalamata

INdAM - GNSAGA Project, codice CUP E53C24001950001

Notation

- $\mathbb{F}_{q^2}$ finite field with q^2 elements
- $\mathcal{X}$ projective, non-singular, geometrically irreducible, algebraic curve defined over $\mathbb{F}_{q^2}$
- $\mathcal{X}(\mathbb{F}_{q^2})$ set of the $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}$
- $g = g(\mathcal{X})$ genus of $\mathcal{X}$, $g = \dfrac{(d-1)(d-2)}{2}$
- $\mathrm{Aut}(\mathcal{X}) = \{\phi : \mathcal{X} \longrightarrow \mathcal{X} \mid \phi \text{ birational}\}$

Quotient curves

Let G be a finite subgroup of $\mathrm{Aut}(\mathcal{X})$, then G acts faithfully on $\mathcal{X}$ and has a finite number of short orbits $\Omega_1, \ldots \Omega_n$.

Definition

The curve $\mathcal{X}/G$ whose points are the G-orbits of $\mathcal{X}$ is called **quotient curve** of $\mathcal{X}$ by G.

Maximal curves

Theorem (Hasse-Weil bound)

Let $\mathcal{X}(\mathbb{F}_{q^2})$ be the number of $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}$, then

$$q^2 + 1 - 2gq \leq |\mathcal{X}(\mathbb{F}_{q^2})| \leq q^2 + 1 + 2gq.$$

Maximal curves

Theorem (Hasse-Weil bound)

Let $\mathcal{X}(\mathbb{F}_{q^2})$ be the number of $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}$, then

$$q^2 + 1 - 2gq \leq |\mathcal{X}(\mathbb{F}_{q^2})| \leq q^2 + 1 + 2gq.$$

Definition

If $\mathcal{X}$ attains the Hasse-Weil upper bound it is called $\mathbb{F}_{q^2}$-*maximal*.

Hermitian curve

Example **Hermitian curve** $\mathcal{H}_q$

Two different models:

$$X^{q+1} - Y^q - Y = 0$$

$$\omega X^{q+1} + Y^q - Y = 0 \quad \omega \in \mathbb{F}_{q^2} \text{ such that } \omega^{q+1} = -1$$

$$g = \frac{q(q-1)}{2}$$

$$|\mathcal{H}_q(\mathbb{F}_{q^2})| = q^3 + 1 = q^2 + 1 + 2gq$$

Hermitian curve

Theorem

$$\mathrm{Aut}(\mathcal{H}_q) \cong \mathrm{PGU}(3, q)$$

Hermitian curve

Theorem

$$\mathrm{Aut}(\mathcal{H}_q) \cong \mathrm{PGU}(3, q)$$

Theorem (Stichtenoth, 1973)

$|\mathrm{Aut}(\mathcal{X})| \leq 16g^4$, *unless* $\mathcal{X}$ *is a Hermitian curve.*

Hermitian curve

Theorem

$$\mathrm{Aut}(\mathcal{H}_q) \cong \mathrm{PGU}(3, q)$$

Theorem (Stichtenoth, 1973)

$|\mathrm{Aut}(\mathcal{X})| \leq 16g^4$, *unless* $\mathcal{X}$ *is a Hermitian curve.*

$\mathrm{PGU}(3, q)$ has plenty of subgroups!

Maximal curves

Theorem (Kleiman-Serre)

If $\mathcal{X}$ is $\mathbb{F}_{q^2}$-maximal and $\mathcal{Y}$ is a quotient curve of $\mathcal{X}$ then $\mathcal{Y}$ is $\mathbb{F}_{q^2}$-maximal.

Maximal curves

Theorem (Kleiman-Serre)

If $\mathcal{X}$ is $\mathbb{F}_{q^2}$-maximal and $\mathcal{Y}$ is a quotient curve of $\mathcal{X}$ then $\mathcal{Y}$ is $\mathbb{F}_{q^2}$-maximal.

Theorem (Ihara 1981)

The largest genus for an $\mathbb{F}_{q^2}$-maximal curve is

$$g = \frac{q(q-1)}{2}.$$

Maximal curves

Theorem (Kleiman-Serre)

If $\mathcal{X}$ is $\mathbb{F}_{q^2}$-maximal and $\mathcal{Y}$ is a quotient curve of $\mathcal{X}$ then $\mathcal{Y}$ is $\mathbb{F}_{q^2}$-maximal.

Theorem (Ihara 1981)

The largest genus for an $\mathbb{F}_{q^2}$-maximal curve is

$$g = \frac{q(q-1)}{2}.$$

Theorem (Rück-Stichtenoth 1994)

If a curve $\mathcal{X}$ is $\mathbb{F}_{q^2}$-maximal and has genus $g = \frac{q(q-1)}{2}$, then

$$\mathcal{X} \cong \mathcal{H}_q.$$

Known results

- Montanucci-Zini (2018)

$$q \equiv 1 \pmod 4$$

Known results

- Montanucci-Zini (2018)

$$q \equiv 1 \pmod 4$$

- García-Stichtenoth-Xing (2000)

Known results

- Montanucci-Zini (2018)

$$q \equiv 1 \pmod 4$$

- García-Stichtenoth-Xing (2000)
- Cossidente-Korchmáros-Torres (2000)

Known results

- Montanucci-Zini (2018)

$$q \equiv 1 \pmod 4$$

- García-Stichtenoth-Xing (2000)
- Cossidente-Korchmáros-Torres (2000)
- Giulietti-Hirschfeld-Korchmáros-Torres (2006)

Known results

- Montanucci-Zini (2018)

$$q \equiv 1 \pmod 4$$

- García-Stichtenoth-Xing (2000)
- Cossidente-Korchmáros-Torres (2000)
- Giulietti-Hirschfeld-Korchmáros-Torres (2006)
- Gatti-Korchmáros (2024)

Known results

- Montanucci-Zini (2018)

$$q \equiv 1 \pmod 4$$

- García-Stichtenoth-Xing (2000)
- Cossidente-Korchmáros-Torres (2000)
- Giulietti-Hirschfeld-Korchmáros-Torres (2006)
- Gatti-Korchmáros (2024)
- Subgroups of order dp, $d \neq p$: this work

GOAL: To determine explicit equations for each quotient curve of $\mathcal{H}_q$ by subgroups G of order dp with $d \neq p$ a prime and $d, p > 3$

GOAL: To determine explicit equations for each quotient curve of $\mathcal{H}_q$ by subgroups G of order dp with $d \neq p$ a prime and $d, p > 3$

Theorem (D.-Gatti 2025)

1. $\mathcal{H}_q/G$ *has genus* $g = \frac{1}{2d}(q-d+1)\left(\frac{q}{p}-1\right)$ *and equation*
$$\sum_{i=0}^{h-1} Y^{p^i} + \omega X^{(q+1)/d} = 0$$
2. $\mathcal{H}_q/G$ *has genus* $g = \frac{q}{2d}\left(\frac{q}{p}-1\right)$ *and equation*
$$\omega X^{(q-1)/d} - Y + X^{2(p-1)/d}Y^p + \cdots + X^{2(p^{h-1}-1)/d}Y^{q/p} = 0$$
3. $\mathcal{H}_q/G$ *has genus* $g = \frac{q}{2dp}(q-1)$ *and equation*
$$\omega\left(\frac{Y^2}{X^d}\right)^{(q-1)/d} + 1 - A(X,Y) = 0 \text{ where}$$
$$A(X,Y) = \sum_{i=0}^{h-1}\sum_{j=0}^{h-1}\left(\frac{Y^2}{X^d}\right)^{(p^i-1)/2d}\left(\frac{Y^2}{X^d}\right)^{(p^j-1)/2d} X^{(p^i+p^j)/2}.$$

Background

- The stabilizer S_{P_∞} of P_∞ in $\mathrm{Aut}(\mathcal{H}_q)$ consists of all maps

$$\psi_{a,b,\lambda} : (x, y) \longmapsto (\lambda x + a, a^q \lambda x + \lambda^{q+1} y + b)$$

$$a \in \mathbb{F}_{q^2}, \quad \lambda \in \mathbb{F}_{q^2}^*, \quad b^q + b = a^{q+1}$$

$$\text{for the model } X^{q+1} - Y^q - Y = 0$$

or

$$\varphi_{a,b,\lambda} : (x, y) \longmapsto (\lambda x + a, a^q \lambda \omega x + \lambda^{q+1} y + b)$$

$$a \in \mathbb{F}_{q^2}, \quad \lambda \in \mathbb{F}_{q^2}^*, \quad b^q - b = -\omega^{q+1}$$

$$\text{for the model } \omega X^{q+1} + Y^q - Y = 0$$

and

$$S_{P_\infty} = S_p \rtimes C.$$

In the former case, $S_p = \left\{ \psi_{a,b,1} \mid b^q + b = a^{q+1},\ a, b \in \mathbb{F}_{q^2} \right\}$ and $C = \left\{ \psi_{0,0,\lambda} \mid \lambda \in \mathbb{F}_{q^2}^* \right\}$.

Background

- The center $Z(S_p)$ of S_p has order q and it consists of all maps $\psi_{0,b,1}$ with $b^q + b = 0$, $b \in \mathbb{F}_{q^2}$
- $Z(S_p)$ is an elementary abelian p-group
- The non-trivial elements of S_p form two conjugacy classes in S_{P_∞} in $\mathrm{Aut}(\mathcal{H}_q)$, one comprises all non-tivial elements of $Z(S_p)$, the other does the remaining $q^3 - q$ elements
- The elements of S_{P_∞} other than those in $Z(S_p)$ have order p or $p^2 = 4$ according as $p > 2$ or $p = 2$
- Let G be a group of order uv where u and v are prime numbers with $u < v$. Then
  - (I) if $u \nmid (v-1)$ G is a cyclic group
  - (II) if $u|(v-1)$ either G is a cyclic group or G is a semidirect product $C_v \rtimes C_u$

Background

Theorem (Cossidente-Korchmáros-Torres 2000)

Let H be a subgroup of $\mathrm{Aut}(\mathcal{H}_q)$ of order p. Then either

(1) $\mathcal{H}_q/H : \sum_{i=1}^{h} \eta^{q/p^i} + \omega\xi^{q+1} = 0$ *with* $\omega^{q-1} = -1$, $g(\mathcal{H}_q/H) = \frac{1}{2}q\left(\frac{q}{p} - 1\right)$, *and H is in the center of a Sylow p-subgroup of* $\mathrm{Aut}(\mathcal{H}_q)$;

(2) $\mathcal{H}_q/H : \eta^q + \eta - (\sum_{i=1}^{h} \xi^{q/p^i})^2 = 0$ *for* $p > 2$, $g(\mathcal{H}_q/H) = \frac{1}{2}\frac{q}{p}(q-1)$, *and H is not in the center of a Sylow p-subgroup of* $\mathrm{Aut}(\mathcal{H}_q)$.

Lemma

A subgroup G of $PGU(3,q)$ of order dp, with $d,p>3$, two different prime integers, is a subroup of the stabilizer of P_∞ and there are three possibilities for G

(I) $G=\Sigma_p\times\Sigma_d$ *with* $\Sigma_p=\langle\varphi_{0,1,1}\rangle$ *and* $\Sigma_d=\langle\varphi_{0,0,\lambda}\rangle$, $\lambda^d=1$, $d|(q+1)$;

(II) $G=\Sigma_p\rtimes\Sigma_d$ *with* $\Sigma_p=\langle\varphi_{0,1,1}\rangle$ *and* $\Sigma_d=\langle\varphi_{0,0,\lambda}\rangle$, $\lambda^d=1$, $d|(p-1)$;

(III) $G=\Sigma_p\rtimes\Sigma_d$ *with* $\Sigma_p=\langle\varphi_{1,\omega/2,1}\rangle$ *and* $\Sigma_d=\langle\varphi_{0,0,\lambda}\rangle$, $\lambda^d=1$, $d|(p-1)$.

Case (I)

Theorem

If G is of the type (I) then $\mathcal{H}_q/G$ has genus

$$g = \frac{1}{2d}(q - d + 1)\left(\frac{q}{p} - 1\right)$$

and equation

$$\sum_{i=0}^{h-1} \tau^{p^i} + \omega\zeta^{(q+1)/d} = 0$$

with $d|(q+1)$.

Case (I)

$$G = \Sigma_p \times \Sigma_d$$

with $\Sigma_p = \langle \varphi_{0,1,1} \rangle$ and $\Sigma_d = \langle \varphi_{0,0,\lambda} \rangle$, $\lambda^d = 1$, $d|(q+1)$

Steps:

1. $\mathcal{H}_q/G \cong (\mathcal{H}_q/\Sigma_p)/(G/\Sigma_p)$
2. $\xi = x$
   $\eta = y^p - y$

$$\varphi_{0,1,1}(\xi) = \xi \text{ and } \varphi_{0,1,1}(\eta) = \eta$$

3. $\mathcal{H}_q/\Sigma_p : \sum_{i=1}^{h} \eta^{p^i} + \omega\xi^{q+1} = 0$

Case (I)

4. $\Sigma_d = \langle \varphi_{0,0,\lambda} \rangle$ with $\lambda \in \mathbb{F}_{q^2}$ $\lambda^d = 1$
5. $\varphi_{0,0,\lambda}$ induces $\varphi : (\xi, \eta) \longrightarrow (\lambda\xi, \eta)$
6. $\Phi_\lambda = \langle \varphi \rangle$
7. $\zeta = \xi^d$ and $\tau = \eta \longrightarrow \mathrm{Fix}(\Phi_\lambda) = \mathbb{F}_{q^2}(\zeta, \tau)$
8. $\sum_{i=1}^{h} \eta^{p^i} + \omega\xi^{q+1} = 0 \longrightarrow \sum_{i=0}^{h-1} \tau^{p^i} + \omega\zeta^{(q+1)/d} = 0$

Case (II)

Theorem

If G is of the type (II) then $\mathcal{H}_q/G$ has genus

$$g = \frac{1}{2}\frac{q}{d}\left(\frac{q}{p} - 1\right)$$

and equation

$$\omega\epsilon^{(q-1)/d} - A(\epsilon, \rho) = 0, \quad d \mid (p-1)$$

where

$$A(\epsilon, \rho) = \rho + \epsilon^{2(p-1)/d}\rho^p + \cdots + \epsilon^{2(p^{h-1}-1)/d}\rho^{q/p}.$$

Case (II)

$$G = \Sigma_p \rtimes \Sigma_d$$

with $\Sigma_p = \langle \varphi_{0,1,1} \rangle$ and $\Sigma_d = \langle \varphi_{0,0,\lambda} \rangle$, $\lambda^d = 1$, $d|(p-1)$

Steps:

1. $\mathcal{H}_q/G \cong (\mathcal{H}_q/\Sigma_p)/(G/\Sigma_p)$
2. $\mathcal{H}_q/\Sigma_p : \sum_{i=1}^{h} \eta^{p^i} + \omega\xi^{q+1} = 0$
3. $\Sigma_d = \langle \varphi_{0,0,\lambda} \rangle$ with $\lambda \in \mathbb{F}_{q^2}$ $\lambda^d = 1$

Case (II)

4. $\varphi_{0,0,\lambda}$ induces $\varphi : (\xi, \eta) \longrightarrow (\lambda\xi, \lambda^2\eta)$
5. $\Phi_\lambda = \langle \varphi \rangle$
6. $\epsilon = \xi^d$ and $\rho = \dfrac{\eta}{\xi^2} \longrightarrow \mathrm{Fix}(\Phi_\lambda) = \mathbb{F}_{q^2}(\epsilon, \rho)$
7. $\displaystyle\sum_{i=1}^{h} \eta^{p^i} + \omega\xi^{q+1} = 0 \longrightarrow \omega\epsilon^{(q-1)/d} - A(\epsilon, \rho) = 0$ where

$$A(\epsilon, \rho) = \rho + \epsilon^{2(p-1)/d}\rho^p + \cdots + \epsilon^{2(p^{h-1}-1)/d}\rho^{q/p}$$

Case (III)

Theorem

If G is of the type (III) then $\mathcal{H}_q/G$ has genus

$$g = \frac{q}{2dp}(q-1)$$

and equation

$$\left(\frac{\tau^2}{\iota^d}\right)^{(q-1)/d} + 1 - A(\iota,\tau) = 0$$

where

$$A(\iota,\tau) = \sum_{i=0}^{h-1}\sum_{j=0}^{h-1}\left(\frac{\tau^2}{\iota^d}\right)^{(p^i-1)/2d}\left(\frac{\tau^2}{\iota^d}\right)^{(p^j-1)/2d}\iota^{(p^i+p^j)/2}.$$

Thank you for your attention!