Galois subcovers of the Hermitian curve in characteristic p with respect to subgroups of order pd with $d \neq p$ prime

Barbara Gatti

University of Salento, Italy

July 20, 2024

joint work with Arianna Dionigi

Introduction

$\mathcal{X}$ projective, absolutely irreducible, non-singular, algebraic curve defined over the finite field $\mathbb{F}_{q^2}$

Studied since **1980s**

- ◇ Coding Theory
- ◇ Cryptography
- ◇ Finite geometry
- ◇ Shift register sequences
- ◇ . . .

Introduction

$\mathcal{X}$ projective, absolutely irreducible, non-singular, algebraic curve defined over the finite field $\mathbb{F}_{q^2}$

Studied since **1980s**

- ◇ Coding Theory
- ◇ Cryptography
- ◇ Finite geometry
- ◇ Shift register sequences
- ◇ ...

$\longrightarrow$ *Maximal Curves*

Maximal Curves

$$\textit{Hasse-Weil upper bound}\ : N(\mathcal{X}) \leq\ 1 + q^2 + 2q\mathfrak{g}$$

$\mathcal{X}$ defined over $\mathbb{F}_{q^2}$ is $\mathbb{F}_{q^2}$-maximal if it attains the *Hasse-Weil upper bound*

$N(\mathcal{X})$ number of $\mathbb{F}_{q^2}$-rational points
$\mathfrak{g}$ genus of the curve $\mathcal{X}$

Maximal Curves

$$\textit{Hasse-Weil upper bound}\ : N(\mathcal{X}) \leq\ 1 + q^2 + 2q\mathfrak{g}$$

$\mathcal{X}$ defined over $\mathbb{F}_{q^2}$ is $\mathbb{F}_{q^2}$-maximal if it attains the *Hasse-Weil upper bound*

$N(\mathcal{X})$ number of $\mathbb{F}_{q^2}$-rational points
$\mathfrak{g}$ genus of the curve $\mathcal{X}$

Examples

1-dimensional Deligne-Lusztig Varieties

◇ *Hermitian* curve - characteristic $p \geq 2$
◇ *Suzuki* curve - characteristic 2
◇ *Ree* curve - characteristic 3

$\mathcal{X}$ algebraic curve over $\mathbb{F}_{q^2}$

Let $G \leq Aut(\mathcal{X})$

Fixed field of G: $\mathcal{X}^G = \{x \in \mathcal{X} \mid g(x) = x \; \forall g \in G\} \leq \mathcal{X}$

$\mathcal{Y}$ model of $\mathcal{X}^G$

Quotient curve : $\mathcal{Y} = \mathcal{X}/G$ covered by $\mathcal{X}$

$$\mathcal{Y} \mapsto \mathcal{X}$$

$$[\mathcal{X} : \mathcal{X}^G] = \mid G \mid$$

Kleiman-Serre

If $\mathcal{X}$ is $\mathbb{F}_{q^2}$-maximal and $\mathcal{Y}$ is $\mathbb{F}_{q^2}$-covered by $\mathcal{X}$ then $\mathcal{Y}$ is $\mathbb{F}_{q^2}$-maximal

Lachaud, Sommes d'eisenstein et nombre de points de certaines courbes algebriques sur les corps finis, C.R. Acad. Sci. Paris Ser., 1987.

Galois covering

Kleiman-Serre

If $\mathcal{X}$ is $\mathbb{F}_{q^2}$-maximal and $\mathcal{Y}$ is $\mathbb{F}_{q^2}$-covered by $\mathcal{X}$ then $\mathcal{Y}$ is $\mathbb{F}_{q^2}$-maximal

Lachaud, Sommes d'eisenstein et nombre de points de certaines courbes algebriques sur les corps finis, C.R. Acad. Sci. Paris Ser., 1987.

Is every $\mathbb{F}_{q^2}$-maximal curve (Galois-)covered by the Hermitian curve $\mathcal{H}_q$?

Kleiman-Serre

If $\mathcal{X}$ is $\mathbb{F}_{q^2}$-maximal and $\mathcal{Y}$ is $\mathbb{F}_{q^2}$-covered by $\mathcal{X}$ then $\mathcal{Y}$ is $\mathbb{F}_{q^2}$-maximal

Lachaud, Sommes d'eisenstein et nombre de points de certaines courbes algebriques sur les corps finis, C.R. Acad. Sci. Paris Ser., 1987.

Is every $\mathbb{F}_{q^2}$-maximal curve (Galois-)covered by the Hermitian curve $\mathcal{H}_q$?

Giulietti-Korchmáros curve (2009)

Quotient curve of the Hermitian curve $\mathcal{H}_q$

$\mathbb{F}_{q^2}$-automorphism group of $\mathcal{H}_q$

Quotient curve of the Hermitian curve $\mathcal{H}_q$

Theorem

$Aut(\mathbb{F}_{q^2}(\mathcal{H}_q)) \cong PGU(3,q)$ *(over the finite field $\mathbb{F}_{q^2}$)*

$PGU(3,q)$ rich of subgroups!

Main questions

I. Determination of the possible genera of maximal curves over a given finite field

II. Determination of explicit equations for maximal curves

III. Classification of maximal curves over a finite field which have the same genus

I. Determination of the possible genera of maximal curves over a given finite field

A. García, H. Stichtenoth, and C.P. Xing, On Subfields of the Hermitian Function Field, *Comp. Math* **120** (2000), 137-170.

I. Determination of the possible genera of maximal curves over a given finite field

A. García, H. Stichtenoth, and C.P. Xing, On Subfields of the Hermitian Function Field, *Comp. Math* **120** (2000), 137-170.

$q \equiv 1 \, mod(4)$

Montanucci, Zini, 2018-2020.

I. Determination of the possible genera of maximal curves over a given finite field

A. García, H. Stichtenoth, and C.P. Xing, On Subfields of the Hermitian Function Field, *Comp. Math* **120** (2000), 137-170.

$q \equiv 1\, mod(4)$

Montanucci, Zini, 2018-2020.

$q \equiv 3\, mod(4)$

Work in progress

Our contributions

II. **Determination of explicit equations for maximal curves**

III. Classification of maximal curves over a finite field which have the same genus

Curves defined by explicit equations

Hirschfeld, Korchmáros, Torres, *Algebraic Curves over a Finite Field*, Princeton Series in Applied Mathematics, Princeton University Press, Princeton, NJ, 2008. xx+696 pp.

Subgroup of order p, p prime

A. Cossidente, G. Korchmáros and F. Torres, Curves of large genus covered by the Hermitian curve, *Comm. Algebra* **28** (2000), 4707–4728.

Subgroup of order p^2, p prime

B. Gatti, G. Korchmáros, *Galois subcovers of the Hermitian curve in characteristic p with respect to subgroups of order p^2*, http://arxiv.org/abs/2307.15192, to appear in Finite Fields and Their Applications

Subgroup of order p, p prime

$$\mathcal{A} : \sum_{i=1}^{h} Y^{q/p^i} + \omega X^{q+1} = 0, \quad \omega^{q-1} = -1, \quad h \geq 2$$

$$\mathcal{B} : Y^q + Y - (\sum_{i=1}^{h} X^{q/p^i})^2 = 0, \quad h \geq 2$$

A. Cossidente, G. Korchmáros and F. Torres, Curves of large genus covered by the Hermitian curve, *Comm. Algebra* **28** (2000), 4707–4728.

Hermitian curve

$\mathcal{H}_q$: $Y^q + Y - X^{q+1}$

Function field: $\mathbb{F}_{q^2}(x, y)$ with $y^q + y - x^{q+1} = 0$

Hermitian curve

$\mathcal{H}_q$: $Y^q + Y - X^{q+1}$

Function field: $\mathbb{F}_{q^2}(x,y)$ with $y^q + y - x^{q+1} = 0$

$\mathcal{H}_q$: $Y^q - Y + \omega X^{q+1}$

Function field: $\mathbb{F}_{q^2}(x,y)$ with $y^q - y + \omega x^{q+1} = 0$

$\omega \in \mathbb{F}_{q^2}, \quad \omega^{q-1} = -1$

S_p Sylow p-subgroup of $Aut(\mathbb{F}_{q^2}(\mathcal{H}_q))$

Y_∞ Unique fixed point of S_p

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

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

or

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

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

$\Rightarrow$ S_p is the Sylow p-subgroup of the stabilizer of Y_∞

Subgroups of order dp

p, d prime $p \neq d$ $p, d > 3$

Subgroups of order dp

p, d prime $p \neq d$ $p, d > 3$

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

Subgroups of order dp

p, d prime $p \neq d$ $p, d > 3$

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

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

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

Quotient curves with respect to a subgroup of order dp

Quotient curve $\mathcal{H} = \mathcal{H}_q / G$

$q = p^h$

p, d prime $p \neq d$ $p, d > 3$

$p > d$

Quotient curves with respect to a subgroup of order dp

I. (The nice case)

If $G = \Sigma_p \times \Sigma_d$ then $\mathcal{H}$ has genus

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

and equation

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

with $\omega^{q-1} = -1 \quad and \quad d \mid (q+1)$

Quotient curves with respect to a subgroup of order dp

II.

If $G = \Sigma_p \rtimes \Sigma_d$ and Σ_p is in the center in a Sylow p-subgroup of G, then $\mathcal{H}$ has genus

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

and equation

$$\omega X^{(q-1)/d} - A(X,Y) = 0$$

with $\omega^{q-1} = -1 \quad \textit{and} \quad d \mid (p-1)$ where

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

Quotient curves with respect to a subgroup of order dp

III.

If $G = \Sigma_p \rtimes \Sigma_d$ but Σ_p is not in the center in a Sylow p-subgroup of G, then $\mathcal{H}$ has genus

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

and equation

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

with $d \mid (p-1)$ where

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

Weierstrass semigroup

$\mathcal{X}$ projective, absolutely irreducible, non-singular, algebraic curve defined over the finite field $\mathbb{F}_{q^2}$

Let $P \in \mathcal{X}$. An integer $n \geq 0$ is called a pole number of P if there is a function $f \in \mathbb{F}_{q^2}(\mathcal{X})$ with $(f)_\infty = nP$. Otherwise n is called a gap number of P

The set $H(P)$ of pole numbers of a point P is a semigroup, called the Weierstrass semigroup at P

Weierstrass semigroup

By the Weierstrass Gap Theorem, if $\mathfrak{g}(\mathcal{X}) > 0$, then for each rational $P \in \mathcal{X}$:

- there are exactly $\mathfrak{g}(\mathcal{X})$ gaps
- 1 is always a gap
- the largest gap is $\leq 2\mathfrak{g}(\mathcal{X}) - 1$

Weierstrass semigroup

By the Weierstrass Gap Theorem, if $\mathfrak{g}(\mathcal{X}) > 0$, then for each rational $P \in \mathcal{X}$:

- there are exactly $\mathfrak{g}(\mathcal{X})$ gaps
- 1 is always a gap
- the largest gap is $\leq 2\mathfrak{g}(\mathcal{X}) - 1$

Main ingredient to construct Algebraic-Geometry codes

Weierstrass semigroup

Let P_∞ be the unique point at infinity of the following two curves

$$\mathcal{A} : \sum_{i=1}^{h} Y^{q/p^i} + \omega X^{q+1} = 0, \quad \omega^{q-1} = -1, \quad h \geq 2$$

$$Nice : \sum_{i=1}^{h} Y^{q/p^i} + \omega X^{(q+1)/d} = 0, \quad \omega^{q-1} = -1, \quad d \mid (q+1)$$

Then the Weierstrass semigroup at P_∞ is generated by

- $\frac{q}{p}$ and $q+1$
- $\frac{q}{p}$ and $\frac{q+1}{d}$

Let P_∞ be the unique point at infinity of the following curve

$$\mathcal{B} : Y^q + Y - (\sum_{i=1}^{h} X^{q/p^i})^2 = 0$$

$\left\{\frac{q}{p}; q+1\right\}$ is a telescopic semigroup

$\Rightarrow$ The Weierstrass semigroup at P_∞ is $H(P_\infty) = \langle \frac{q}{p}, q+1 \rangle$

Non-Gaps

$$Eq.II.\ \omega X^{(q-1)/d} - A(X,Y) = 0$$

with $\omega^{q-1} = -1 \quad and \quad d \mid (p-1)$ where

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

$\Rightarrow \frac{q}{p}, \frac{q-1}{d} \in H(P_\infty)$

$$Eq.III.\ \left(\frac{Y^2}{X^d}\right)^{(q-1)/d} + 1 - A(X,Y) = 0$$

with $d \mid (p-1)$ where

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

$\Rightarrow \frac{2(q-1)}{d}, q-1 \in H(P_\infty)$

Applications

$\mathcal{X}$: Algebraic curves over $\mathbb{F}_{q^2} \to \mathcal{C}$: Algebraic Geometry codes

$\mathcal{D}$, $\mathcal{G}$ divisors on $\mathcal{X}$

$\mathcal{D} = P_1 + \cdots + P_r$, P_i $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}$

Applications

$\mathcal{X}$: Algebraic curves over $\mathbb{F}_{q^2} \to \mathcal{C}$: Algebraic Geometry codes

$\mathcal{D}$, $\mathcal{G}$ divisors on $\mathcal{X}$

$\mathcal{D} = P_1 + \cdots + P_r$, P_i $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}$

Designed minimum distance

$$d \geq n - deg(\mathcal{G})$$

Taking $\mathcal{G} = mP \rightarrow$ then knowledge of the gaps at P_∞ may allow one to show that the minimum distance d^* of the code $\mathcal{C}$ may be better than the designed minimum distance d.

A. Garcia, S. J. Kim, R. F. Lax, Consecutive Weierstrass gaps and minimum distance of Goppa codes, J. Pure Appl. Algebra 84 (1993), 199-207.

H. Janwa, On the parameters of algebraic geometric codes, in *Applied algebra, algebraic algorithms and error-correcting codes* (New Orleans, LA, 1991), 19–28, Lecture Notes in Comput. Sci., **539**, Springer, Berlin, 1991.

Applications

t consecutive gaps at P_∞ gives a minimum distance d^* of the code at least t greater than the designed minimum distance d.

A. Garcia, S. J. Kim, R. F. Lax, Consecutive Weierstrass gaps and minimum distance of Goppa codes, *J. Pure Appl. Algebra* **84** (1993), 199-207.

To do

Investigate large intervals of gaps at the point P_∞ of the $\mathbb{F}_{q^2}$-maximal curves considered in the present paper

Example: The nice curve

$$\mathcal{X} : \sum_{i=0}^{h-1} Y^{p^i} + \omega X^{(q+1)/d} = 0$$

$p = 7; d = 5$

$h = 2 \Rightarrow q = p^h = 49 \Rightarrow d \mid (q+1) \qquad \mathfrak{g} = 27$

Non gaps at P_∞:

$$\frac{q}{p} = 7 \text{ and } \frac{q+1}{d} = 10$$

Gap sequence at P_∞:

$1, 2, 3, 4, 5, 6, 8, 9, 11, 12, 13, 15, 16, 18, 19, 22, 23, 25, 26, 29, 32,$
$33, 36, 39, 43, 46, 53.$

Example

For $\gamma = 13$ and $t = 2$

γ: the greater gap at P_∞ of the gaps sequence interval
$t+1$: the lenght of the gaps sequence interval considered

$$d^* = \mid \mathcal{D} \mid - \gamma + t + 1 = 5037$$

$$d = \mid \mathcal{D} \mid - \gamma = 5034$$