Maximal Curves Over Finite Fields

Barbara Gatti

University of Salento, Italy
University of Basilicata, Italy

5TH PYTHAGOREAN CONFERENCE

3 June 2023

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
- ◇ . . .

$\mathcal{X}$ 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*

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

$\mathcal{X}$ 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 $\mathcal{X}$

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

$\mathcal{X}$ 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

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

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.

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)

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

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 and their classification over a finite field

III. Better understanding of the upper spectrum of genera of $\mathbb{F}_{q^2}$-maximal curves

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

Today contributions

II. Determination of explicit equations for maximal curves and their classification over a finite filed

(Arianna's Talk)

III. **Better understanding of the upper spectrum of genera of $\mathbb{F}_{q^2}$-maximal curves**

The Spectrum of genera of Maximal curves

- $\frac{1}{2}q(q-1)$ $\quad$ $\mathcal{H}_q : Y^q + Y - X^{q+1} = 0$

  (Hermitian)

The Spectrum of genera of Maximal curves

$\frac{1}{2}q(q-1)$ $\qquad$ $\mathcal{H}_q: Y^q + Y - X^{q+1} = 0$

(Hermitian)

$\lfloor \frac{1}{4}(q-1)^2 \rfloor$ $\qquad$ $\epsilon_1: Y^q + Y - X^{(q+1)/2} = 0$

q odd

(Fuhrmann-Garcia-Torres, 1997)

$\mathcal{T}_2: X^{q+1} + Tr(Y) = 0$

q even

(Abdòn-Torres, 1999)

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

$\mathcal{H}_q : Y^q + Y - X^{q+1} = 0$

(Hermitian)

$\lfloor \frac{1}{4}(q-1)^2 \rfloor$

$\epsilon_1 : Y^q + Y - X^{(q+1)/2} = 0$

q odd

(Fuhrmann-Garcia-Torres, 1997)

$\mathcal{T}_2 : X^{q+1} + Tr(Y) = 0$

q even

(Abdòn-Torres, 1999)

$\lfloor \frac{1}{6}(q^2 - q + 4) \rfloor$

- $\mathcal{F}_0 : X^{(q+1)/3} + X^{2(q+1)/3} + Y^{q+1} = 0, \quad q \equiv_3 2$
- $\mathcal{G} : Y^q - YX^{2(q-1)/3} + X^{(q-1)/3} = 0, \quad q \equiv_3 1$
- $\mathcal{T}'_3 : (Y + Y^3 + \ldots + Y^{q/3})^2 - X^q - X = 0, \quad q \equiv_3 0$

Third largest genus

$$\mathcal{F}_0 : X^{(q+1)/3} + X^{2(q+1)/3} + Y^{q+1} = 0 \qquad q \equiv 2\ mod(3)$$

P. Beelen, M. Montanucci, L. Vicino, Weierstrass semigroups and automorphism group of a maximal curve with the third largest genus, Finite Fields and Their Applications, 92 (2023), p. 102300., 2018-2020.

- Weierstrass semi-groups
- Automorphism group

Fourth largest genus

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

$\lfloor \frac{1}{4}(q-1)^2 \rfloor$

$\lfloor \frac{1}{6}(q^2-q+4) \rfloor$

$\boxed{\lfloor \frac{1}{8}(q^2-2q+5) \rfloor}$

Fourth largest genus

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

$\lfloor \frac{1}{4}(q-1)^2 \rfloor$

$\lfloor \frac{1}{6}(q^2-q+4) \rfloor$

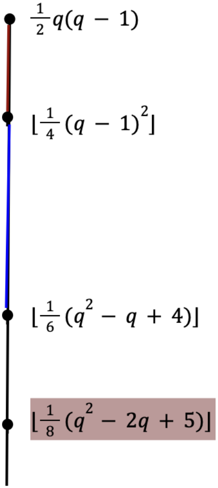
$\lfloor \frac{1}{8}(q^2-2q+5) \rfloor$

Gatti - Korchmáros (2023)

$$q \equiv 0 \; mod(4)$$

Garcia-Stichtenoth-Xing (1998)

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



Gatti - Korchmáros (2023)

$$q \equiv 0 \; mod(4)$$

Garcia-Stichtenoth-Xing (1998)

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

Missing explicit equation

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

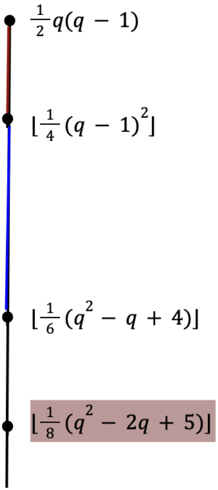
$\frac{1}{2}q(q-1)$

$\lfloor \frac{1}{4}(q-1)^2 \rfloor$

$\lfloor \frac{1}{6}(q^2-q+4) \rfloor$

$\lfloor \frac{1}{8}(q^2-2q+5) \rfloor$

Fourth largest genus

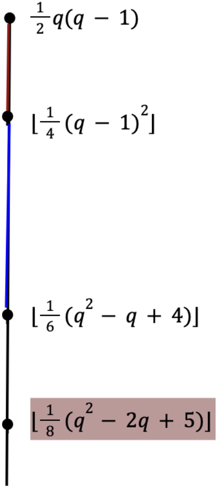


$$q \equiv_4 1 \qquad \to \qquad \mathfrak{g}_4 = \frac{1}{8}(q-1)^2$$

$$X^{(q^2-1)/4} - Y(Y+1)^{q-1} = 0$$

Garcia-Stichtenoth-Xing (1998)

Fourth largest genus



$$q \equiv_4 1 \qquad \rightarrow \qquad \mathfrak{g}_4 = \tfrac{1}{8}(q-1)^2$$

$$X^{(q^2-1)/4} - Y(Y+1)^{q-1} = 0$$

Garcia-Stichtenoth-Xing (1998)

Birationally equivalent plane model

$\mathcal{C} : Y^q + YX^{(q-1)/2} - X^{q-(q-1)/4} = 0$

Function field of $\mathcal{C}$: $\mathbb{F}_{q^2}(x,y)$, where $f(x,y) = y^q + yx^{(q-1)/2} - x^{q-(q-1)/4}$

Singular points of the curve $\mathcal{C}$

$$\mathcal{C} : Y^q + YX^{(q-1)/2} - X^{q-(q-1)/4} = 0$$

$\mathcal{O} = (0:0:1)$

$\mathcal{P}_\infty = (1:0:0)$

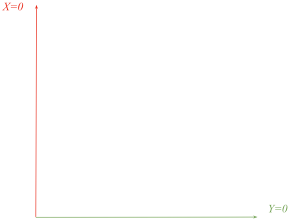
Singular points of the curve $\mathcal{C}$

$$\mathcal{C} : Y^q + YX^{(q-1)/2} - X^{q-(q-1)/4} = 0$$

$\mathcal{O} = (0:0:1)$

$\mathcal{P}_\infty = (1:0:0)$

$$m_{\mathcal{O}}(\mathcal{C}) = \tfrac{1}{2}(q+1)$$
$$l_1 : X = 0; l_2 : Y = 0$$

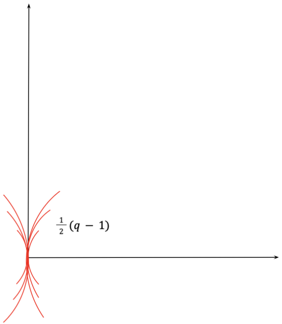


$$\mathcal{C} : Y^q + YX^{(q-1)/2} - X^{q-(q-1)/4} = 0$$

$$\mathcal{O} = (0:0:1)$$

$$\mathcal{P}_\infty = (1:0:0)$$

$$m_{\mathcal{O}}(\mathcal{C}) = \tfrac{1}{2}(q+1)$$
$$l_1 : X = 0; l_2 : Y = 0$$



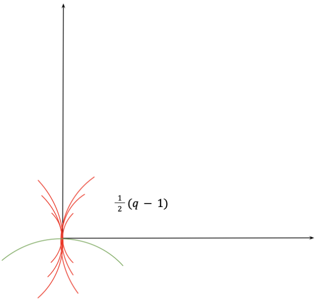
Singular points of the curve $\mathcal{C}$

$$\mathcal{C} : Y^q + YX^{(q-1)/2} - X^{q-(q+1)/4} = 0$$

$\mathcal{O} = (0:0:1)$

$\mathcal{P}_\infty = (1:0:0)$

$$m_{\mathcal{O}}(\mathcal{C}) = \tfrac{1}{2}(q+1)$$
$$l_1 : X = 0; l_2 : Y = 0$$



Singular points of the curve $\mathcal{C}$

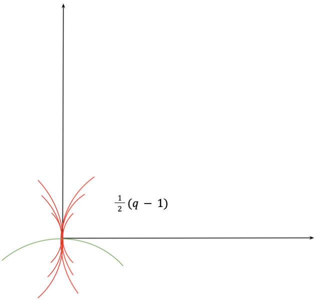
$$\mathcal{C} : Y^q + YX^{(q-1)/2} - X^{q-(q+1)/4} = 0$$

$\mathcal{O} = (0:0:1)$

$$m_{\mathcal{O}}(\mathcal{C}) = \frac{1}{2}(q+1)$$
$$l_1 : X = 0; l_2 : Y = 0$$

$\mathcal{P}_\infty = (1:0:0)$

$$m_{\mathcal{P}_\infty}(\mathcal{C}) = \frac{1}{4}(q-1)$$
$$l_\infty$$



Singular points of the curve $\mathcal{C}$

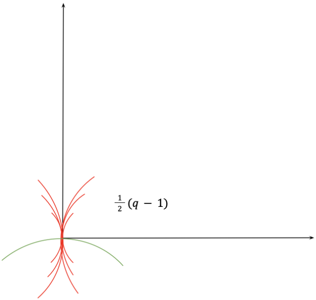
$$\mathcal{C} : Y^q + YX^{(q-1)/2} - X^{q-(q+1)/4} = 0$$

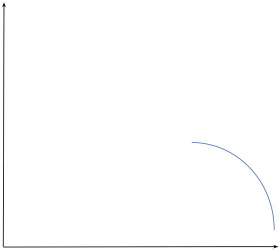
$\mathcal{O} = (0:0:1)$

$$m_{\mathcal{O}}(\mathcal{C}) = \tfrac{1}{2}(q+1)$$
$$l_1 : X = 0;\ l_2 : Y = 0$$

$\mathcal{P}_\infty = (1:0:0)$

$$m_{\mathcal{P}_\infty}(\mathcal{C}) = \tfrac{1}{4}(q-1)$$
$$l_\infty$$





Natural Embedding Theorem

$\mathcal{D} := (q+1)P$ Frobenius divisor of the curve $\mathcal{C}$, $P \in \mathcal{C}(\mathbb{F}_{q^2})$

The Riemann-Roch spaces $\mathcal{L}(\mathcal{D})$ defines a
birational embedding

$$\omega : \mathcal{C} \to PG(r, q^2)$$

$r = dim(\mathcal{L}(\mathcal{D})) - 1 \quad$ (Frobenius dimension)

Korchmáros - Torres (2001)

Every $\mathbb{F}_{q^2}$-maximal curve is isomorphic over $\mathbb{F}_{q^2}$ to a curve of $PG(r, q^2)$ of degree $q+1$ lying on a non-degenerate Hermitian variety $\mathcal{H}_{r,q}$ defined over $\mathbb{F}_{q^2}$.

◇ The arising curve in non-singular

Natural Embeddig Theorem

$P = P_\infty \in \mathcal{C}(\mathbb{F}_{q^2})$ and $\mathcal{D} = (q+1)P_\infty$

Riemann-Roch space of $\mathcal{D}$

$$\mathcal{L}(\mathcal{D}) = \left\langle 1, x, y, \frac{y^2}{x}, \left(\frac{y^2}{x}\right)^2 \right\rangle$$

$\Rightarrow r = 4 \quad$ (Frobenius dimension)

Natural Embeddig Theorem

$P = P_\infty \in \mathcal{C}(\mathbb{F}_{q^2})$ and $\mathcal{D} = (q+1)P_\infty$

Riemann-Roch space of $\mathcal{D}$

$$\mathcal{L}(\mathcal{D}) = \left\langle 1, x, y, \frac{y^2}{x}, \left(\frac{y^2}{x}\right)^2 \right\rangle$$

$\Rightarrow r = 4$ (Frobenius dimension)

Coordinate functions of the Frobenius embedding φ

$$\begin{array}{rrcl} & PG(2,q^2) & & PG(4,q^2) \\ \varphi : & \mathcal{C} & \rightarrow & \mathcal{X} \\ & (1,x,y) & \mapsto & \left(1, x, y, \frac{y^2}{x}, \left(\frac{y^2}{x}\right)^2\right) \end{array}$$

Natural Embeddig

The curve $\mathcal{X}$ lies on the non-degenerate Hermitian variety

$$\mathcal{H}_4 : -X_1^{q+1} + 4X_2^{q+1} - 2X_3^{q+1} + X_0X_4^q + X_0^qX_4 = 0$$

Natural Embeddig

The curve $\mathcal{X}$ lies on the non-degenerate Hermitian variety

$$\mathcal{H}_4 : -X_1^{q+1} + 4X_2^{q+1} - 2X_3^{q+1} + X_0X_4^q + X_0^qX_4 = 0$$

The curve $\mathcal{X}$ lies on the two quadrics

$$\Sigma_1 : X_3^2 = X_0X_4$$

$$\Sigma_2 : X_2^2 = X_1X_3$$

Natural Embeddig

The curve $\mathcal{X}$ lies on the non-degenerate Hermitian variety

$$\mathcal{H}_4 : -X_1^{q+1} + 4X_2^{q+1} - 2X_3^{q+1} + X_0X_4^q + X_0^qX_4 = 0$$

The curve $\mathcal{X}$ lies on the two quadrics

$$\Sigma_1 : X_3^2 = X_0X_4$$

$$\Sigma_2 : X_2^2 = X_1X_3$$

$\Rightarrow$ $\mathcal{X}$ is the complete intersection of $\mathcal{H}_4 \cap \Sigma_1 \cap \Sigma_2$

Non-Gaps of $\mathcal{C}$ at P_∞

$P_\infty \in \mathcal{C}(\mathbb{F}_{q^2})$
$\mathcal{D} = (q+1)P_\infty$

$div(x)_\infty = qP_\infty$

$div\left(\frac{y^2}{x}\right)_\infty = \left(\frac{q+1}{2}\right) P_\infty$

$div(y)_\infty = \left(q - \frac{q-1}{4}\right) P_\infty$

$div\left(\frac{y^2}{x}\right)^2_\infty = (q+1)P_\infty$

The non-gaps at P_∞ less than or equal to $q+1$

$$\frac{1}{2}(q+1) < q - \frac{q-1}{4} < q < q+1$$

Non-Gaps of $\mathcal{C}$ at P_∞

$P_\infty \in \mathcal{C}(\mathbb{F}_{q^2})$
$\mathcal{D} = (q+1)P_\infty$

$div(x)_\infty = qP_\infty$

$div(y)_\infty = \left(q - \frac{q-1}{4}\right) P_\infty$

$div\left(\frac{y^2}{x}\right)_\infty = \left(\frac{q+1}{2}\right) P_\infty$

$div\left(\frac{y^2}{x}\right)^2_\infty = (q+1)P_\infty$

The non-gaps at P_∞ less than or equal to $q+1$

$$\frac{1}{2}(q+1) < q - \frac{q-1}{4} < q < q+1$$

◇ The generators of the Weierstrass semigroup $H(P_\infty)$ still missing...

Automorphism group

$$\mathcal{C} = \mathcal{H}_q/\Phi \quad \text{(Quotient curve)}$$

$\Phi = \langle \varphi_\lambda \rangle, \mid \Phi \mid = 4$ (Cyclic subgroup)

$$\varphi_\lambda : (X, Y) \to (\lambda X, \lambda^2 Y), \quad \lambda^4 = 1$$

Automorphism group

$$\mathcal{C} = \mathcal{H}_q/\Phi \quad \text{(Quotient curve)}$$

$\Phi = \langle \varphi_\lambda \rangle, \mid \Phi \mid = 4$ (Cyclic subgroup)

$\varphi_\lambda : (X, Y) \to (\lambda X, \lambda^2 Y), \quad \lambda^4 = 1$

$Aut(\mathcal{C}) \supset G, \mid G \mid = \frac{q^2-1}{2}$

$$\mathcal{C} = \mathcal{H}_q/\Phi \quad \text{(Quotient curve)}$$

$\Phi = \langle \varphi_\lambda \rangle, \mid \Phi \mid = 4$ (Cyclic subgroup)

$\varphi_\lambda : (X, Y) \to (\lambda X, \lambda^2 Y), \quad \lambda^4 = 1$

$Aut(\mathcal{C}) \supset G, \mid G \mid = \frac{q^2-1}{2}$

Generators of G

$$G := \langle \Psi, \Theta \rangle$$

$\Psi : (x, y) \to (\theta x, \theta^{(q+3)/4} y)$, where $\theta^{(q^2-1)/4} = 1$
$\Theta : (x, y) \to \left(\frac{x^3}{y^4}, \frac{x^2}{y^3} \right)$

Θ is non-linear $\Rightarrow$ $Aut(\mathcal{C})$ is non-linear

Automorphism group

Frobenius embedding φ

$$\begin{aligned}\varphi: \quad \mathcal{C} &\to \mathcal{X}\\ (1,x,y) &\mapsto \left(1,x,y,\frac{y^2}{x},\left(\frac{y^2}{x}\right)^2\right)\end{aligned}$$

- $Aut(\mathcal{X})$ is linear
- $Aut(\mathcal{X})$ preserves $\mathcal{H}_4$
- $Aut(\mathcal{X})$ preserves the pencil generated by Σ_1 and Σ_2

Frobenius embedding φ

$$\begin{aligned} \varphi : \quad\quad \mathcal{C} &\to \mathcal{X} \\ (1,x,y) &\mapsto \left(1,x,y,\frac{y^2}{x},\left(\frac{y^2}{x}\right)^2\right) \end{aligned}$$

- $\diamond$ $Aut(\mathcal{X})$ is linear
- $\diamond$ $Aut(\mathcal{X})$ preserves $\mathcal{H}_4$
- $\diamond$ $Aut(\mathcal{X})$ preserves the pencil generated by Σ_1 and Σ_2

G is the Automorphism group of the curve $\mathcal{C}$

$G = Aut(\mathcal{C})$, where $G = \langle \Psi, \Theta \rangle$

$\Rightarrow$ Inherited from $Aut(\mathcal{H}_q)$

Bibliography

B. Gatti, G. Korchmáros, Galois subcovers of the Hermitian curve in characteristic p with respect to subgroups of order p^2, *Finite Fields and Their Applications*, **98**, (2024).

B. Gatti, G. Schulte, On a Galois subcover of the Hermitian curve of genus $\mathfrak{g} = \frac{1}{8}(q-1)^2$, arXiv:2410.22037, (2024).