\mathbb{F}_{p^2} -maximal curves with many automorphisms are Galois-covered by the Hermitian curve

Daniele Bartoli

Università degli Studi di Perugia (Italy)

(Joint work with Maria Montanucci and Fernando Torres)

Finite Geometries - Fifth Irsee Conference 10-16 September 2017

Outline

- Maximal curves
- 2 \mathbb{F}_{p^2} -maximal curves with many automorphisms: main result
- 3 The Fricke-MacBeath curve over finite fields and the \mathbb{F}_{11^2} -maximal Wiman's sextic
- 4 Related questions

Notation and terminology

• $\mathcal{X}\subseteq \mathbb{P}^r(\bar{\mathbb{F}}_q)$ projective, geometrically irreducible, non-singular algebraic curve defined over \mathbb{F}_q

• g genus of \mathcal{X}

If
$$r=2$$
 then $g=\frac{(d-1)(d-2)}{2}$ where $d=deg(\mathcal{X})$

$$ullet$$
 $\mathcal{X}(\mathbb{F}_q)=\mathcal{X}\cap\mathbb{P}^r(\mathbb{F}_q)$

Maximal Curves

 \mathcal{X} defined over \mathbb{F}_q

Hasse-Weil Bound

$$|\mathcal{X}(\mathbb{F}_q)| \leq q + 1 + 2g\sqrt{q}$$

Definition

$${\mathcal X}$$
 is ${\mathbb F}_q$ -maximal if $|{\mathcal X}({\mathbb F}_q)|=q+1+2g\sqrt{q}$

Example

Hermitian curve:

$$\mathcal{H}_q: X^q+X=Y^{q+1}, \quad q=p^h$$
 $g=q(q-1)/2, \quad Aut(\mathcal{H}_q)\cong PGU(3,q), \quad |\mathcal{H}_q(\mathbb{F}_{q^2})|=q^3+1$

Rational maps and pull-back

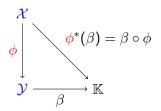
$$\mathcal{X} \subseteq \mathbb{P}^r(\mathbb{K})$$
 and $\mathcal{Y} \subseteq \mathbb{P}^s(\mathbb{K})$

• Function field of \mathcal{X}

$$\mathbb{K}(\mathcal{X}) = \left\{ rac{F + \mathbb{I}}{G + \mathbb{I}} \mid G \notin \mathbb{I} = \mathbb{I}(\mathcal{X})
ight\}$$

• Rational map $\phi: \mathcal{X} \to \mathcal{Y}$: is a map given by rational functions

$$\phi = (\alpha_0 : \dots : \alpha_s), \text{ for almost all } P \in \mathcal{X}$$



Coverings and Galois-coverings

 ${\mathcal Y}$ is covered by ${\mathcal X}$ if there exists a non-constant rational map

$$\phi: \mathcal{X} \to \mathcal{Y}$$

 $\mathbb{K}(\mathcal{X})$: $\phi^*(\mathbb{K}(\mathcal{Y}))$ is a finite field extension

$$\mathcal{Y}$$
 is a Galois-covered by $\mathcal{X} \iff \mathbb{K}(\mathcal{X}) : \phi^*(\mathbb{K}(\mathcal{Y}))$
Galois extension

Basic properties of coverings

```
\begin{array}{ccc} \mathcal{X} \ \mathbb{F}_q\text{-maximal} \\ \phi: \mathcal{X} \to \mathcal{Y} \ \text{non-constant} &\Longrightarrow & \mathcal{Y} \ \text{is} \ \mathbb{F}_q\text{-maximal} \\ \text{rational map defined over} \ \mathbb{F}_q \end{array}
```

Basic properties of coverings

```
\begin{array}{ccc} \mathcal{X} \ \mathbb{F}_q\text{-maximal} \\ \phi: \mathcal{X} \to \mathcal{Y} \ \text{non-constant} &\Longrightarrow & \mathcal{Y} \ \text{is} \ \mathbb{F}_q\text{-maximal} \\ \text{rational map defined over} \ \mathbb{F}_q \end{array}
```

- C non-singular algebraic curve
- ullet G finite automorphism group acting on ${\mathcal C}$
- \mathcal{X} quotient curve of \mathcal{C} by G

Basic properties of coverings

 $\begin{array}{ccc} \mathcal{X} \ \mathbb{F}_q\text{-maximal} \\ \pmb{\phi}: \mathcal{X} \to \mathcal{Y} \ \text{non-constant} &\Longrightarrow & \mathcal{Y} \ \text{is} \ \mathbb{F}_q\text{-maximal} \\ \text{rational map defined over} \ \mathbb{F}_q & & & & & & & & & & & & \\ \end{array}$

- C non-singular algebraic curve
- ullet G finite automorphism group acting on ${\mathcal C}$
- \mathcal{X} quotient curve of \mathcal{C} by G

Riemann-Hurwitz Formula

$$2g(C) - 2 = |G|(2g(X) - 2) + D$$



• $g(\mathcal{X}) \leq g_1 = \frac{q(q-1)}{2}$ (Ihara, 1981)

•
$$g(X) \le g_1 = \frac{q(q-1)}{2}$$
 (*Ihara*, 1981)

•
$$g = g_1 \Longrightarrow \mathcal{X} \cong \mathcal{H}_q$$
 (Rück – Stichtenoth, 1994)

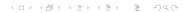
- $g(X) \le g_1 = \frac{q(q-1)}{2}$ (*Ihara*, 1981)
- $g = g_1 \Longrightarrow \mathcal{X} \cong \mathcal{H}_q$ (Rück Stichtenoth, 1994)
- 2006: Curve \mathbb{F}_{q^2} -maximal curve not Galois-covered by \mathcal{H}_q (Garcia, Stichtenoth) $\to \mathbb{F}_{27^2}$ -maximal curve

- $g(X) \le g_1 = \frac{q(q-1)}{2}$ (*Ihara*, 1981)
- $g = g_1 \Longrightarrow \mathcal{X} \cong \mathcal{H}_q$ (Rück Stichtenoth, 1994)
- 2006: Curve \mathbb{F}_{q^2} -maximal curve not Galois-covered by \mathcal{H}_q (Garcia, Stichtenoth) $\to \mathbb{F}_{27^2}$ -maximal curve
- 2009: Family fo \mathbb{F}_{q^2} -maximal curves not covered by \mathcal{H}_q (Giulietti, Korchmáros) $\to \mathbb{F}_{q^6}$ -maximal curve

- $g(X) \le g_1 = \frac{q(q-1)}{2}$ (*Ihara*, 1981)
- $g = g_1 \Longrightarrow \mathcal{X} \cong \mathcal{H}_q$ (Rück Stichtenoth, 1994)
- 2006: Curve \mathbb{F}_{q^2} -maximal curve not Galois-covered by \mathcal{H}_q (Garcia, Stichtenoth) $\to \mathbb{F}_{27^2}$ -maximal curve
- 2009: Family fo \mathbb{F}_{q^2} -maximal curves not covered by \mathcal{H}_q (Giulietti, Korchmáros) $\to \mathbb{F}_{q^6}$ -maximal curve

Question

Is there an \mathbb{F}_{p^2} -maximal curve not covered by the Hermitian curve?



- $g(X) \le g_1 = \frac{q(q-1)}{2}$ (*Ihara*, 1981)
- $g = g_1 \Longrightarrow \mathcal{X} \cong \mathcal{H}_q$ (Rück Stichtenoth, 1994)
- 2006: Curve \mathbb{F}_{q^2} -maximal curve not Galois-covered by \mathcal{H}_q (Garcia, Stichtenoth) $\to \mathbb{F}_{27^2}$ -maximal curve
- 2009: Family fo \mathbb{F}_{q^2} -maximal curves not covered by \mathcal{H}_q (Giulietti, Korchmáros) $\to \mathbb{F}_{q^6}$ -maximal curve

Question

Is there an \mathbb{F}_{p^2} -maximal curve not covered by the Hermitian curve? Is there an \mathbb{F}_{p^2} -maximal curve not Galois-covered by the Hermitian curve?



Situation up to p = 5

• p=2,3: trivial (Every \mathbb{F}_{p^2} -maximal curve is Galois-covered by \mathcal{H}_p)

Situation up to p = 5

- p=2,3: trivial (Every \mathbb{F}_{p^2} -maximal curve is Galois-covered by \mathcal{H}_p)
- p=5: Every \mathbb{F}_{25} -maximal curve is Galois-covered by \mathcal{H}_5

Situation up to p = 5

- p=2,3: trivial (Every \mathbb{F}_{p^2} -maximal curve is Galois-covered by \mathcal{H}_p)
- p=5: Every \mathbb{F}_{25} -maximal curve is Galois-covered by \mathcal{H}_5 $M(5):=\{g(\mathcal{X})\mid \mathcal{X} \text{ is } \mathbb{F}_{25}\text{-maximal}\}=\{0,1,2,3,4,10\}$

- **3** $g(\mathcal{X}) = 3 \iff \mathcal{X} \cong \mathcal{Y}_3 : y^6 = x^5 + 2x^4 + 3x^3 + 4x^2 + 3xy^3$
- **6** $g(\mathcal{X}) = 1 \iff \mathcal{X} \cong \mathcal{Y}_1 : x^3 + y^3 + 1 = 0$

Almost all the known examples of maximal curves not Galois-covered by \mathcal{H}_q have large automorphism group



We investigated curves with $|Aut(\mathcal{X})| > 84(g(\mathcal{X}) - 1)$

Almost all the known examples of maximal curves not Galois-covered by \mathcal{H}_q have large automorphism group

 \downarrow

We investigated curves with $|Aut(\mathcal{X})| > 84(g(\mathcal{X}) - 1)$

Theorem (B.-Montanucci-Torres, 2017)

 \mathcal{X} \mathbb{F}_{p^2} -maximal curve, $p \geq 7$, $g(\mathcal{X}) \geq 2$,

$$|\mathrm{Aut}(\mathcal{X})| > 84(g(\mathcal{X}) - 1) \Longrightarrow \mathcal{X}$$
 Galois-covered by \mathcal{H}_p

Almost all the known examples of maximal curves not Galois-covered by \mathcal{H}_q have large automorphism group

 \Downarrow

We investigated curves with $|Aut(\mathcal{X})| > 84(g(\mathcal{X}) - 1)$

Theorem (B.-Montanucci-Torres, 2017)

 \mathcal{X} \mathbb{F}_{p^2} -maximal curve, $p \geq 7$, $g(\mathcal{X}) \geq 2$,

$$|\mathrm{Aut}(\mathcal{X})|>84(g(\mathcal{X})-1)\Longrightarrow \mathcal{X}$$
 Galois-covered by \mathcal{H}_p

• (B. Gunby, A. Smith, A. Yuan, 2015): \mathcal{X} defined over \mathbb{F}_{p^2} , $p \geq 7$, $g(\mathcal{X}) \geq 2$, $|Aut(\mathcal{X})| \geq \max\{84(g-1), g^2\}$ $\Rightarrow \mathcal{X} \cong \mathcal{X}_m : y^m = x^p - x$

 $(\mathcal{X}_m \text{ is not } \mathbb{F}_{n^2}\text{-maximal for each } m \dots)$

Theorem (B.-Montanucci-Torres, 2017)

$$\mathcal{X}$$
 \mathbb{F}_{p^2} -maximal curve, $p \geq 7$, $g(\mathcal{X}) \geq 2$,
$$|\mathrm{Aut}(\mathcal{X})| > 84(g(\mathcal{X}) - 1) \Longrightarrow \mathcal{X}$$
 Galois-covered by \mathcal{H}_p

Theorem (B.-Montanucci-Torres, 2017)

$$\mathcal{X}$$
 \mathbb{F}_{p^2} -maximal curve, $p \geq 7$, $g(\mathcal{X}) \geq 2$,
$$|\mathrm{Aut}(\mathcal{X})| > 84(g(\mathcal{X}) - 1) \Longrightarrow \mathcal{X}$$
 Galois-covered by \mathcal{H}_p

• An \mathbb{F}_{p^2} -maximal "GK-curve" cannot exist

Theorem (B.-Montanucci-Torres, 2017)

$$\mathcal{X}$$
 \mathbb{F}_{p^2} -maximal curve, $p \geq 7$, $g(\mathcal{X}) \geq 2$, $|\operatorname{Aut}(\mathcal{X})| > 84(g(\mathcal{X}) - 1) \Longrightarrow \mathcal{X}$ Galois-covered by \mathcal{H}_p

• An \mathbb{F}_{p^2} -maximal "GK-curve" cannot exist

• Find \mathbb{F}_{p^2} -maximal curves not Galois-covered by the Hermitian curve

• Can we extend it to $|\operatorname{Aut}(\mathcal{X})| \leq 84(g-1)$?



Sketch of the proof

Lemma

$$\begin{array}{l} \mathcal{X} \ \mathbb{F}_{p^2}\text{-maximal curve} \\ \mathcal{X} \not\cong_{\mathbb{F}_{p^2}} \mathcal{H}_p \\ G \leq Aut(\mathcal{X}), \ p \mid |G| \end{array}$$

$$\implies p^2 \nmid |G|$$

Sketch of the proof

Lemma

$$\mathcal{X} \ \mathbb{F}_{p^2}$$
-maximal curve $\mathcal{X} \not\cong_{\mathbb{F}_{p^2}} \mathcal{H}_p \implies p^2 \nmid |G|$ $G \leq Aut(\mathcal{X}), \ p \mid |G|$

Theorem (Garcia-Tafazolian, 2008)

- $q = p^h$, $\mathcal{X} \mathbb{F}_{q^2}$ -maximal curve
- $\exists H \leq \operatorname{Aut}(\mathcal{X})$ abelian, |H| = q, \mathcal{X}/H rational

$$\exists m \mid q+1$$
 : $\mathcal{X} \cong_{\mathbb{F}_{q^2}} \mathcal{H}_m : x^q + x = y^m$

Sketch of the proof

Lemma

$$\begin{array}{ccc} \mathcal{X} \ \mathbb{F}_{p^2}\text{-maximal curve} \\ \mathcal{X} \not\cong_{\mathbb{F}_{p^2}} \mathcal{H}_p & \Longrightarrow & p^2 \nmid |G| \\ G \leq Aut(\mathcal{X}), \ p \mid |G| \end{array}$$

Theorem (Garcia-Tafazolian, 2008)

- $q = p^h$, $\mathcal{X} \mathbb{F}_{q^2}$ -maximal curve
- $\exists H \leq \operatorname{Aut}(\mathcal{X})$ abelian, |H| = q, \mathcal{X}/H rational

$$\exists m \mid q+1$$
 : $\mathcal{X} \cong_{\mathbb{F}_{q^2}} \mathcal{H}_m : x^q + x = y^m$

 \mathcal{H}_m is covered by $\mathcal{H}_q: x^q + x = y^{q+1}$:

$$\mathcal{H}_m \cong \mathcal{H}_p/G, \qquad G = \{\varphi_{\lambda} : (x,y) \mapsto (x,\lambda y) \mid \lambda^{(q+1)/m} = 1\}$$



• $g(\mathcal{C}) \geq 2 \Longrightarrow |\mathrm{Aut}(\mathcal{C})| < \infty$ (Schmid, Iwasawa-Tamagawa, Roquette, Rosentlich, Garcia)

•
$$g(\mathcal{C}) \geq 2 \Longrightarrow |\mathrm{Aut}(\mathcal{C})| < \infty$$
 (Schmid, Iwasawa-Tamagawa, Roquette, Rosentlich, Garcia)

•
$$p=0,\ g(\mathcal{C})\geq 2\Longrightarrow |\mathrm{Aut}(\mathcal{C})|\leq 84(g-1)$$
 (Hurwitz)

•
$$g(\mathcal{C}) \geq 2 \Longrightarrow |\mathrm{Aut}(\mathcal{C})| < \infty$$
 (Schmid, Iwasawa-Tamagawa, Roquette, Rosentlich, Garcia)

•
$$p = 0$$
, $g(\mathcal{C}) \ge 2 \Longrightarrow |\operatorname{Aut}(\mathcal{C})| \le 84(g-1)$

(Hurwitz)

Example: Klein quartic:
$$K: X^3 + Y + XY^3 = 0$$
, $g = 3$, $Aut(K) = PSL(2,7)$, $|Aut(K)| = 168 = 84(3-1)$

•
$$g(\mathcal{C}) \geq 2 \Longrightarrow |\mathrm{Aut}(\mathcal{C})| < \infty$$
 (Schmid, Iwasawa-Tamagawa, Roquette, Rosentlich, Garcia)

•
$$p=0,\ g(\mathcal{C})\geq 2\Longrightarrow |\mathrm{Aut}(\mathcal{C})|\leq 84(g-1)$$
 (Hurwitz)

Example: Klein quartic:
$$K: X^3 + Y + XY^3 = 0$$
, $g = 3$, $Aut(K) = PSL(2,7)$, $|Aut(K)| = 168 = 84(3-1)$

• $gcd(p, |Aut(C)|) = 1 \Longrightarrow |Aut(C)| \le 84(g-1)$



What if
$$|Aut(\mathcal{X})| \leq 84(g-1)$$
?

- p > 0: No classifications of Hurwitz groups |G| = 84(g-1)
- Partial classification if \mathcal{X} is classical (Schoeneberg's Lemma)

What if
$$|Aut(\mathcal{X})| \leq 84(g-1)$$
?

- p > 0: No classifications of Hurwitz groups |G| = 84(g-1)
- Partial classification if \mathcal{X} is classical (Schoeneberg's Lemma)

Lemma (B.-Montanucci-Torres, 2017)

$$p \geq 7$$
, \mathcal{X} \mathbb{F}_{p^2} -maximal, $g(\mathcal{X}) \geq 2$
 $40(g(\mathcal{X}) - 1) < |\mathrm{Aut}(\mathcal{X})| \leq 84(g(\mathcal{X}) - 1)$

Then \mathcal{X} is Galois-covered by \mathcal{H}_p unless $g(\mathcal{X}/\mathrm{Aut}(\mathcal{X}))=0$ and

$$\bullet \ p \geq 11, \quad (|O_1|, |O_2|, |O_3|) = \left(\frac{|\operatorname{Aut}(\mathcal{X})|}{2}, \frac{|\operatorname{Aut}(\mathcal{X})|}{3}, \frac{|\operatorname{Aut}(\mathcal{X})|}{7}\right)$$

$$\bullet \qquad (|O_1|,|O_2|,|O_3|) = \left(\frac{|\operatorname{Aut}(\mathcal{X})|}{2},\frac{|\operatorname{Aut}(\mathcal{X})|}{3},\frac{|\operatorname{Aut}(\mathcal{X})|}{8}\right)$$



• g = 3: Klein quartic unique example up to isomorphisms

- g = 3: Klein quartic unique example up to isomorphisms
- (R. Fricke, 1899): The next example occurs for g = 7

- g = 3: Klein quartic unique example up to isomorphisms
- (R. Fricke, 1899): The next example occurs for g = 7
- (A. M. MacBeath, 1965): Explicit equations realizing Fricke's example as an algebraic curve. Uniqueness over $\mathbb C$

- g = 3: Klein quartic unique example up to isomorphisms
- (R. Fricke, 1899): The next example occurs for g = 7
- (A. M. MacBeath, 1965): Explicit equations realizing Fricke's example as an algebraic curve. Uniqueness over $\mathbb C$
- (R. Hidalgo, 2015): Affine plane model, attribuited to Bradley Brock, over $\mathbb Q$

$$\mathcal{F}: 1 + 7xy + 21x^2y^2 + 35x^3y^3 + 28x^4y^4 + 2x^7 + 2y^7 = 0$$



- g = 3: Klein quartic unique example up to isomorphisms
- (R. Fricke, 1899): The next example occurs for g = 7
- (A. M. MacBeath, 1965): Explicit equations realizing Fricke's example as an algebraic curve. Uniqueness over $\mathbb C$
- (R. Hidalgo, 2015): Affine plane model, attribuited to Bradley Brock, over Q

$$\mathcal{F}: 1 + 7xy + 21x^2y^2 + 35x^3y^3 + 28x^4y^4 + 2x^7 + 2y^7 = 0$$

• (J. Top, C. Verschoor, 2016): Criterion to count the points of the Fricke-MacBeath curve over finite fields



The Fricke-MacBeath curve

Proposition (Top-Verschoor, 2016)

$$p \equiv \pm 1 \pmod{14}$$

$${\mathcal F}$$
 is ${\mathbb F}_{p^2}$ -maximal \iff $y^2=(x^3+x^2-114x-127)$ is ${\mathbb F}_{p^2}$ -maximal

The Fricke-MacBeath curve

Proposition (Top-Verschoor, 2016)

$$p \equiv \pm 1 \pmod{14}$$

$$\mathcal{F}$$
 is \mathbb{F}_{p^2} -maximal \iff $y^2 = (x^3 + x^2 - 114x - 127)$ is \mathbb{F}_{p^2} -maximal

 \mathcal{F} \mathbb{F}_{p^2} -maximal for infinitely many p

MAGMA: \mathcal{F} is \mathbb{F}_{p^2} -maximal for $p \in \{71, 251, 503, 2591\}$ and $\operatorname{Aut}(\mathcal{X}) \cong PSL(2, 8)$

The Fricke-MacBeath curve

Proposition (Top-Verschoor, 2016)

$$p \equiv \pm 1 \pmod{14}$$

$${\mathcal F}$$
 is ${\mathbb F}_{p^2}$ -maximal \iff $y^2=(x^3+x^2-114x-127)$ is ${\mathbb F}_{p^2}$ -maximal

 $\mathcal{F} \mathbb{F}_{p^2}$ -maximal for infinitely many p

MAGMA: \mathcal{F} is \mathbb{F}_{p^2} -maximal for $p \in \{71, 251, 503, 2591\}$ and $\operatorname{Aut}(\mathcal{X}) \cong \mathit{PSL}(2, 8)$

Theorem (B.-Montanucci-Torres, 2017)

For p = 71 \mathcal{F} is not a Galois subcover of \mathcal{H}_{71}

Question

Is this \mathbb{F}_{p^2} -maximal curve covered by the Hermitian curve \mathcal{H}_p ?

Question

Is this \mathbb{F}_{p^2} -maximal curve covered by the Hermitian curve \mathcal{H}_p ?

ullet Negative answer $\,\,
ightarrow$

Question

Is this \mathbb{F}_{p^2} -maximal curve covered by the Hermitian curve \mathcal{H}_p ?

ullet Negative answer $\,\,
ightarrow$

Theorem (B.-Montanucci-Torres, 2017)

$$\mathcal{X} \mathbb{F}_{p^2}$$
-maximal curve, $p \geq 7$, $g(\mathcal{X}) \geq 2$,

$$|\operatorname{Aut}(\mathcal{X})| > 84(g(\mathcal{X}) - 1) \Longrightarrow \mathcal{X}$$
 Galois-covered by \mathcal{H}_p

Question

Is this \mathbb{F}_{p^2} -maximal curve covered by the Hermitian curve \mathcal{H}_p ?

ullet Negative answer $\,\,
ightarrow$

Theorem (B.-Montanucci-Torres, 2017)

$$\mathcal{X} \ \mathbb{F}_{p^2}$$
-maximal curve, $p \ge 7$, $g(\mathcal{X}) \ge 2$,

$$|\mathrm{Aut}(\mathcal{X})|>84(g(\mathcal{X})-1)\Longrightarrow\mathcal{X}$$
 Galois-covered by \mathcal{H}_p

Question

Is this \mathbb{F}_{p^2} -maximal curve covered by the Hermitian curve \mathcal{H}_p ?

ullet Negative answer $\,\,
ightarrow$

Theorem (B.-Montanucci-Torres, 2017)

$$\mathcal{X}$$
 \mathbb{F}_{p^2} -maximal curve, $p \geq 7$, $g(\mathcal{X}) \geq 2$, $|\operatorname{Aut}(\mathcal{X})| > 84(g(\mathcal{X}) - 1) \Longrightarrow \mathcal{X}$ Galois-covered by \mathcal{H}_p

• Positive answer \to First example of an \mathbb{F}_{q^2} -maximal curve which is covered but not Galois-covered by \mathcal{H}_q



Thank you for your attention