BULLETIN OF THE BRAZILIAN MATHEMATICAL SOCIETY

Bull Braz Math Soc, New Series 37(1), 139-152

A maximal curve which is not a Galois subcover of the Hermitian curve

Arnaldo Garcia* and Henning Stichtenoth

Abstract. We present a maximal curve of genus 24 defined over $\mathbb{F}_{q^2}$ with $q = 27$, that is not a Galois subcover of the Hermitian curve.

Keywords: rational points, finite fields, maximal curves, Galois coverings, Hermitian curves.

Mathematical subject classification: 11G20, 11D45, 14H25.

1 Introduction

Let $K = \mathbb{F}_{q^2}$ denote the finite field with q^2 elements. By a curve over $\mathbb{F}_{q^2}$ we will mean a projective nonsingular algebraic curve defined over K, and irreducible over the algebraic closure $\overline{\mathbb{F}}_q$. A curve $\mathcal{C}$ over $\mathbb{F}_{q^2}$ is said to be *K-maximal* if the cardinality of the set $\mathcal{C}(\mathbb{F}_{q^2})$ of its $\mathbb{F}_{q^2}$-rational points attains the Hasse-Weil upper bound; i.e.,

$$\#\mathcal{C}(\mathbb{F}_{q^2}) = q^2 + 1 + 2q \cdot g(\mathcal{C}),$$

where $g(\mathcal{C})$ denotes the genus of $\mathcal{C}$.

Maximal curves are interesting in connection with Coding Theory, automorphism groups, finite geometries, Stöhr-Voloch theory of Frobenius-orders, etc. (see for example [14], [15], [16], [17]).

Ihara [8] showed that if $\mathcal{C}$ is $\mathbb{F}_{q^2}$-maximal, then its genus satisfies:

$$g(\mathcal{C}) \leq \frac{q(q-1)}{2}.$$

Received 30 November 2005.

*The author was partially supported by CNPq-Brazil (470193/03-4) and by PRONEX (CNPq-FAPERJ).

The most interesting maximal curve over $\mathbb{F}_{q^2}$ is the so-called Hermitian curve $\mathcal{H}$ which can be given by the following affine equation:

$$Z^q + Z = X^{q+1} \quad \text{over} \quad K = \mathbb{F}_{q^2}.$$

The genus of $\mathcal{H}$ satisfies

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

and it is the unique maximal curve over $\mathbb{F}_{q^2}$ with the genus given as above (see [12]).

We say that a curve $\mathcal{Y}$ covers another curve χ over $\mathbb{F}_{q^2}$ if we have a surjective map

$$\varphi\colon \mathcal{Y} \to \chi$$

where both curves and the map are all defined over $\mathbb{F}_{q^2}$. Serre (see [10]) showed that if $\mathcal{Y}$ is K-maximal, then the curve χ is also K-maximal.

Several classes of maximal curves have been investigated (see for example [1], [2], [5], [12]) and it turned out that they are all covered by the Hermitian curve. Also, Korchmáros and Torres (see [9]) showed that all maximal curves lie on Hermitian varieties. So a basic question is the following:

Question. *Is any maximal curve $\mathcal{C}$ over $\mathbb{F}_{q^2}$ a subcover of the Hermitian curve $\mathcal{H}$; i.e., is there always a surjective map $\varphi\colon \mathcal{H} \to \mathcal{C}$ defined over K?*

The aim here is to present a maximal curve $\mathcal{C}_3$ of genus 24 over $\mathbb{F}_{q^2}$ (with $q = 27$) which is not a Galois subcover of $\mathcal{H}$; i.e., there is no surjective Galois map φ defined over K (see Theorem 3)

$$\varphi\colon \mathcal{H} \to \mathcal{C}_3.$$

The curve $\mathcal{C}_3$ above is the curve given by the affine equation

$$y^9 - y = x^7 \quad \text{over} \quad \mathbb{F}_{27^2}. \tag{1.1}$$

This curve $\mathcal{C}_3$ is inside a family of $\mathbb{F}_{q^2}$-maximal curves, where $q = \ell^3$ is a cubic power (see Theorem 1).

2 Certain maximal curves

In his lecture at AGCT-10, J.-P. Serre has introduced the following affine equation for a maximal curve $\mathcal{C}_2$ over $\mathbb{F}_{q^2}$ with $q = 8$:

$$y^4 + y = x^3 \quad \text{over} \quad \mathbb{F}_{64}. \tag{2.1}$$

The Hermitian curve $\mathcal{H}$ over $\mathbb{F}_{64}$ is given by

$$Z^8 + Z = X^9,$$

and the substitutions $z = Z^2 + Z$ and $x = X^3$ give us the following subcover of the Hermitian curve:

$$z^4 + z^2 + z = x^3. \tag{2.2}$$

The curves in (2.1) and (2.2) are both of genus 3 and they are not isomorphic to each other. This raises the question whether the Hermitian $\mathcal{H}$ covers the curve $\mathcal{C}_2$? Surprisingly enough it is shown in [7] that there is a Galois covering map $\mathcal{H} \to \mathcal{C}_2$ of degree 9 and moreover we have an intermediate curve $\mathcal{Y}$ such that

$$\mathcal{H} \xrightarrow{\psi} \mathcal{Y} \xrightarrow{\varphi} \mathcal{C}_2$$

with $\deg \psi = 3$ and $\deg \varphi = 3$, and the map φ above is unramified.

First we generalize the curve $\mathcal{C}_2$ given by Equation (2.1) as follows:

Theorem 1. *Consider the curve $\mathcal{C}_\ell$ over $\mathbb{F}_{q^2}$ with $q = \ell^3$ given by*

$$y^{\ell^2} - y = x^{\ell^2 - \ell + 1}.$$

Then the curve $\mathcal{C}_\ell$ is $\mathbb{F}_{q^2}$-maximal with genus $g(\mathcal{C}_\ell) = \frac{(\ell^2-1)(\ell^2-\ell)}{2}$.

Proof. The assertion about the genus is trivial. We have only to show that

$$\#\mathcal{C}_\ell(\mathbb{F}_{q^2}) = 1 + \ell^6 + (\ell^2 - 1)(\ell^2 - \ell) \cdot \ell^3.$$

We rewrite the equality above as follows:

$$\#\mathcal{C}_\ell(\mathbb{F}_{q^2}) = (1 + \ell^2) + \ell^2 \cdot (\ell^2 - 1)(\ell^2 - \ell + 1) \cdot (\ell + 1).$$

The number $(1+\ell^2)$ above comes from the unique point at infinity and the points on $\mathcal{C}_\ell$ with $x = 0$. So we have to show that there are exactly

$$\ell^2 \cdot (\ell^2 - 1)(\ell^2 - \ell + 1) \cdot (\ell + 1)$$

rational points on $\mathcal{C}_\ell$ with a nonzero first coordinate. Since $\mathbb{F}_{\ell^2} \subseteq \mathbb{F}_{\ell^6} = \mathbb{F}_{q^2}$ we see that each such first coordinate gives rise to ℓ^2 rational points on $\mathcal{C}_\ell$ (i.e., gives rise to ℓ^2 corresponding second coordinates). So we have to show that

$$\#\{x \in \mathbb{F}_{q^2}^* \mid \exists\ y \in \mathbb{F}_{q^2} \text{ with } (x, y) \in \mathcal{C}_\ell\} = (\ell^2 - 1)(\ell^2 - \ell + 1) \cdot (\ell + 1).$$

By Hilbert's Satz 90 we are led to consider the trace of the extension $\mathbb{F}_{q^2}$ over $\mathbb{F}_{\ell^2}$; i.e., we have to look for solutions $x \in \mathbb{F}_{q^2}^*$ of the trace

$$\left(x^{\ell^2-\ell+1}\right)^{\ell^4} + \left(x^{\ell^2-\ell+1}\right)^{\ell^2} + x^{\ell^2-\ell+1} = 0.$$

Since $x \neq 0$, we must have

$$\left(x^{(\ell^2-\ell+1)(\ell^2-1)}\right)^{\ell^2+1} + x^{(\ell^2-\ell+1)(\ell^2-1)} + 1 = 0.$$

Let H denote the multiplicative subgroup of $\mathbb{F}_{q^2}^*$ with order

$$|H| = \ell^2 + \ell + 1.$$

For $x \in \mathbb{F}_{q^2}^*$ and $w = x^{(\ell^2-\ell+1)(\ell^2-1)}$, we must have that $w \in H$. So we have to show that

$$\#\{w \in H \ ; \ w^{\ell^2+1} + w + 1 = 0\} = \ell + 1.$$

Since $w \in H$ we have $w^{\ell^2+1} = \frac{1}{w^\ell}$ and hence for $w \in H$, we get that

$$w^{\ell^2+1} + w + 1 = \frac{w^{\ell+1} + w^\ell + 1}{w^\ell}.$$

Now one checks that $w^{\ell+1} + w^\ell + 1 = 0$ implies that $w \in H$. □

Remark 1. The curves given by Eqs. (1.1) and (2.1) are the particular cases given by $\ell = 3$ and $\ell = 2$ in Theorem 1, respectively.

We show in the next section that the curve $\mathcal{C}_3$ with genus $g = 24$ given by the affine equation $y^9 - y = x^7$ is not a Galois subcover of the Hermitian curve $\mathcal{H}$ over $\mathbb{F}_{q^2}$ with $q = 27$. For the proof of this claim we will need the following result:

Theorem 2. *Let $\mathcal{H}$ denote the Hermitian curve over $K = \mathbb{F}_{q^2}$ and let $p = Char(K)$. Suppose that $\varphi\colon \mathcal{H} \to \chi$ is a Galois cover over K, denote by H the corresponding Galois group and write*

$$|H| = \deg\varphi = m \cdot p^u \text{ with } gcd(m, p) = 1.$$

If there is a fully ramified point for the map φ and

$$q^2 - q + 1 \not\equiv 0 \pmod{\deg\varphi},$$

then the genus of the quotient curve χ is given by

$$g(\chi) = \frac{q - p^w}{2m \cdot p^u}(q - (d-1) \cdot p^v),$$

where $d = gcd(m, q+1)$ and where v and w are natural numbers attached to the group H and $v + w = u$. Moreover if $m = 1$, then there is exactly one fully ramified point for the morphism φ.

Proof. The case $m = 1$ follows from Proposition 2.2 and Section 3 of [6] and the case $m > 1$ follows from Theorem 4.4 of [6]. □

3 Maximal curves $\mathcal{C}$ with genus 24

The Hermitian curve $\mathcal{H}$ over $\mathbb{F}_{q^2}$ with $q = 27$ has genus $g(\mathcal{H}) = 351$ and it can be given by the equation:

$$Z^{27} + Z = X^{28}.$$

Let $\mathcal{C}$ be any maximal curve of genus 24 over $\mathbb{F}_{q^2}$ with $q = 27$. Suppose we have a Galois covering map φ of degree d:

$$\varphi \colon \mathcal{H} \xrightarrow{d} \mathcal{C}.$$

We must have that $d \leq 15$ since

$$2g(\mathcal{H}) - 2 \geq d \cdot (2g(\mathcal{C}) - 2).$$

We have also that $d \geq 10$, as follows from the bound

$$\#\mathcal{H}(\mathbb{F}_{27^2}) \leq d \cdot \#\mathcal{C}(\mathbb{F}_{27^2}).$$

We are therefore left with the possibilities:

$$d = 10, 11, 12, 13, 14, 15.$$

Cases $d = 11$ or $d = 13$. These possibilities for the degree d of the Galois covering φ are easily discarded. Since d is a prime number, we should have from Hurwitz genus formula:

$$2g(\mathcal{H}) - 2 = d \cdot (2g(\mathcal{C}) - 2) + N \cdot (d-1), \tag{3.1}$$

where N denotes the number of ramified points of the Galois covering. But Equation (3.1) leads to a value of N which is not a natural number in both cases $d = 11$ and $d = 13$.

Cases $d = 10$ or $d = 15$. These cases are also easily discarded, since the prime number 5 does not divide the order of $\mathcal{A}$, where $\mathcal{A}$ denotes the automorphism group of the Hermitian. We have (see [6] and [15]):

$$|\mathcal{A}| = q^3(q^3+1)(q^2-1) \quad \text{and hence} \quad |\mathcal{A}| \not\equiv 0 \bmod 5, \text{ for } q = 27.$$

Remark 2. Notice that $d = 11$ also does not divide $|\mathcal{A}|$ and this shows again that we can discard the case $d = 11$. In case $d = 13$, we have that a 13-Sylow subgroup H of $\mathcal{A}$ has order equal to 13 and Equation (3.1) shows in particular that the quotient curve $\mathcal{H}/H$ is not a curve with genus 24. From Theorem 2 we have the genus formula $g(\mathcal{H}/H) = 27$.

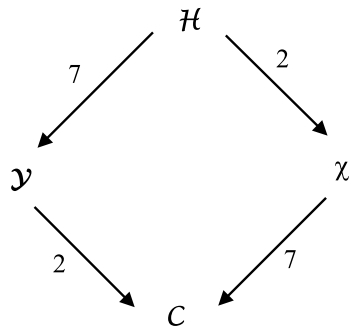
We are left with the two following possibilities for the degree $d := \deg \varphi$

$$\text{Case } d = 14 \quad \text{and} \quad \text{Case } d = 12.$$

Case $d = 14$. We have a Galois covering map (with Galois group denoted by G):

$$\varphi\colon \mathcal{H} \to \mathcal{C} \quad \text{over} \quad K = \mathbb{F}_{q^2} \quad \text{with} \quad q = 27,$$

where $\deg \varphi = |G| = 14$ and $\mathcal{C}$ is a maximal curve over K of genus 24. Let H denote the unique subgroup of G with order $|H| = 7$ and denote by $\mathcal{Y} = \mathcal{H}/H$ the corresponding quotient curve. We have the following picture:



where χ is the unique curve (up to isomorphisms) having index 2 in the Hermitian (see [4] and [5]). An equation and the genus of the curve χ are given by:

$$Z^{27} + Z = x^{14} \quad \text{and} \quad g(\chi) = 169.$$

Notice that $g(\chi) = 169$ can also be obtained from Theorem 2. For that one uses the fact that the automorphisms of order 2 of the Hermitian curve have fixed points.

The degree 7 map $\chi \xrightarrow{7} \mathcal{C}$ is not Galois. Otherwise we would have

$$336 = 2g(\chi) - 2 = 7 \cdot (2g(\mathcal{C}) - 2) + 6N = 322 + 6N,$$

which is not possible.

This shows that $G = D_7$ is the dihedral group of order 14 generated by two elements σ and τ with order $(\sigma) = 2$, order $(\tau) = 7$ and the relations $\sigma\tau^i = \tau^{-i}\sigma$ for $i = 1, 2, \ldots, 6$. We have $H = \langle\tau\rangle$ and the elements of order 2 in G are the elements in the set below

$$G \setminus H = \{\sigma\tau^i \mid i \in \mathbb{N} \text{ and } 0 \leq i \leq 6\}.$$

We now consider two subcases:

Subcase 1. The map $\mathcal{H} \xrightarrow{7} \mathcal{Y}$ is ramified.

Since for $q = 27$ we have

$$703 = q^2 - q + 1 \not\equiv 0 (\text{mod } 7),$$

we get from Theorem 2 the following genus formula:

$$g(\mathcal{Y}) = \frac{27 - 1}{2 \times 7}(27 - 6) = 39.$$

This is not possible since we would then have

$$76 = 2g(\mathcal{Y}) - 2 \geq 2 \cdot (2g(\mathcal{C}) - 2) = 92.$$

Subcase 2. The map $\mathcal{H} \xrightarrow{7} \mathcal{Y}$ is unramified.

In this case every point $P \in \mathcal{H}$ that is ramified under the Galois morphism $\varphi\colon \mathcal{H} \to \mathcal{C}$ must have ramification index $e(P) = 2$. Hurwitz genus formula for the map φ gives that we have exactly 56 ramified points P as above. Indeed

$$700 = 2g(\mathcal{H}) - 2 = 14(2g(\mathcal{C}) - 2) + 56.$$

Each element $\sigma\tau^i$ (for $i = 0, 1, \ldots, 6$) of order 2 has exactly 28 fixed points on the Hermitian curve $\mathcal{H}$. This follows from Hurwitz formula applied to the double covering $\mathcal{H} \xrightarrow{2} \chi$. But since $\mathcal{H} \xrightarrow{7} \mathcal{Y}$ is unramified we have that the involutions $\sigma\tau^i$ and $\sigma\tau^j$ for $0 \leq i < j \leq 6$, do not have a common fixed point. Indeed suppose $Q \in \mathcal{H}$ satisfies

$$\sigma\tau^i(Q) = Q = \sigma\tau^j(Q).$$

Then applying σ, we get in particular

$$\tau^i(Q) = \tau^j(Q) \quad \text{and} \quad \tau^{j-i}(Q) = Q.$$

This is impossible since τ^{j-i} generates the same group H as the element τ and hence it cannot have a fixed point Q on $\mathcal{H}$.

But then we would have:

$$7 \times 28 \text{ ramified points for the map } \varphi.$$

So we have also discarded the case $d = 14$.

Remark 3. For each odd divisor n of $(q+1)$ there exists a Galois and unramified covering of degree n

$$\mathcal{H} \xrightarrow{n} \mathcal{Y}.$$

This covering is associated to a Hilbert class field of the curve $\mathcal{Y}$ (see [7], [11] and [13]).

In our situation above (Subcase 2) we have

$$n = 7, \quad q = 27 \quad \text{and} \quad g(\mathcal{Y}) = 51.$$

Suppose we have a double covering $\mathcal{Y} \xrightarrow{2} \mathcal{Y}_1$ making $\mathcal{H}$ a Galois covering of $\mathcal{Y}_1$ with degree 14. From the arguments in Subcase 2 above we have

$$700 = 2g(\mathcal{H}) - 2 \geq 14(2g(\mathcal{Y}_1) - 2) + 7 \times 28$$

and hence we get $g(\mathcal{Y}_1) \leq 19$.

Case $d = 12$. From [4] we have just two Galois subcovers of the Hermitian $\mathcal{H}$ (up to isomorphisms) with index 3. They are:

- The curve $\mathcal{C}_0$ with $g(\mathcal{C}_0) = 108$ given by

$$Y^9 - Y^3 + Y = X^{28}. \tag{3.2}$$

Here the automorphism of $\mathcal{H}$ of order 3 can be chosen as

$$\sigma(X) = X \text{ and } \sigma(Z) = Z + a \text{ with } a^{27} + a = 0.$$

- The curve $\mathcal{C}_1$ with $g(\mathcal{C}_1) = 117$ given by

$$y^{27} + y = (x^9 + x^3 + x)^2. \tag{3.3}$$

  Here the automorphism of $\mathcal{H}$ of order 3 can be chosen as

$$\sigma(X) = X + 1 \text{ and } \sigma(Z) = Z + X - 1.$$

  One can also derive the genus possibilities $g = 108$ (case $v = 0$ and $w = 1$) and $g = 117$ (case $v = 1$ and $w = 0$) from Proposition 3.1 of [6]. (See also Theorem 2 here with $m = 1$).

Let G denote the Galois group of the Galois covering $\varphi\colon \mathcal{H} \to \mathcal{C}$. So the order of G satisfies $|G| = 12 = 4 \times 3$. We consider two subcases:

Subcase 1. G has a normal subgroup H of order 3.

We have here two possibilities:

Subcase 1.1. The quotient curve $\mathcal{H}/H$ is isomorphic to the curve $\mathcal{C}_0$ above (see Equation (3.2)) with genus 108.

Since H is normal in G, then the covering below of degree 4

$$\mathcal{C}_0 \xrightarrow{4} \mathcal{C}$$

is a Galois covering. We can then go from $\mathcal{C}_0$ to the curve $\mathcal{C}$ by inserting an intermediate curve $\mathcal{Y}$:

$$\mathcal{C}_0 \xrightarrow{2} \mathcal{Y} \xrightarrow{2} \mathcal{C}.$$

The unique automorphism σ of order 2 on the curve $\mathcal{C}_0$ satisfies

$$\sigma(X) = -X \quad \text{and} \quad \sigma(Y) = Y.$$

Hence the inserted curve $\mathcal{Y}$ above is given by the equation below

$$Y^9 - Y^3 + Y = x^{14}.$$

Again the unique automorphism σ_1 of order 2 on the curve $\mathcal{Y}$ satisfies

$$\sigma_1(x) = -x \quad \text{and} \quad \sigma_1(Y) = Y.$$

Hence the curve $\mathcal{C}$ of genus 24 can be given by the equation

$$Y^9 - Y^3 + Y = x_1^7 \quad \text{over} \quad \mathbb{F}_{27^2}.$$

The assertions concerning the uniqueness of the automorphisms σ and σ_1 above can be proved with arguments similar to the ones in the proof of Theorem 3 at the end of this paper.

Subcase 1.2. The quotient curve $\mathcal{H}/H$ is isomorphic to the curve $\mathcal{C}_1$ above (see Equation (3.3)) with genus 117.

It is easily seen that the point at infinity of the Hermitian (see Section 3 of [6]) is the only ramified point of the cover $\mathcal{H} \stackrel{3}{\longrightarrow} \mathcal{C}_1$.

Since $\mathcal{C}_1 \stackrel{4}{\longrightarrow} \mathcal{C}$ is a Galois covering we conclude that the degree 12 Galois map $\varphi\colon \mathcal{H} \stackrel{12}{\longrightarrow} \mathcal{C}$ has a fully ramified point. Now Theorem 2 with $v = 1$ and $w = 0$ gives the genus formula:

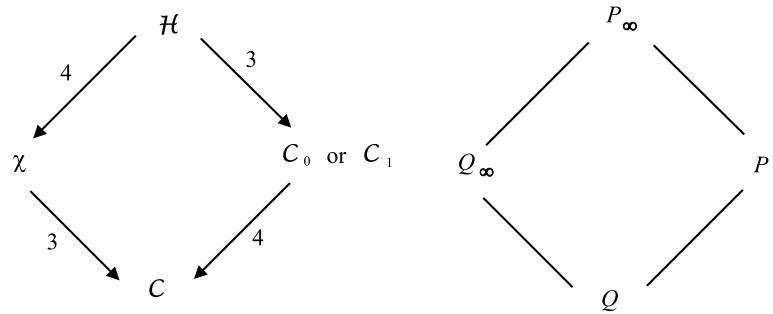
$$g(\mathcal{C}) = \frac{27-1}{8\times 3}(27 - 3\times 3) = \frac{26\times 18}{24} = 19,5$$

which is not possible. So this Subcase 1.2 does not occur.

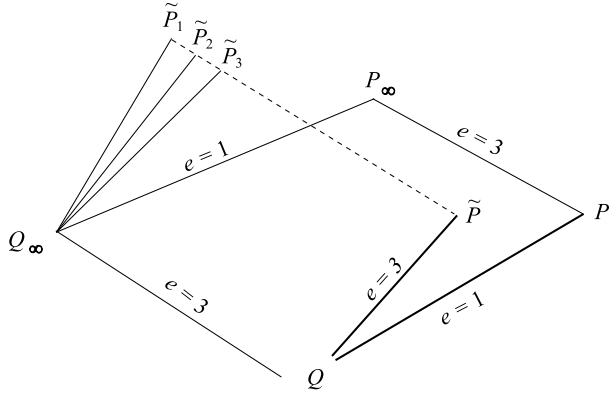
Subcase 2. A subgroup H of order 3 is not normal in G.

It follows from Hilbert's different formula (higher ramification groups) that there is no fully ramified point for the Galois covering $\varphi\colon \mathcal{H} \stackrel{12}{\longrightarrow} \mathcal{C}$. Indeed, if P is fully ramified then $G_1(P) \lhd G_0(P) = G$ and $|G_1(P)| = 3$, where $G_i(P)$ denotes the i-th ramification group.

The group G in this case is isomorphic to the alternating group A_4. Consider the following diagram (where χ denotes the quotient curve by the Klein subgroup of A_4):



where P_∞ is the only ramified point of $\mathcal{H}$ over $\mathcal{C}_i$ ($i = 0$ or $i = 1$) and Q_∞, P and Q denote its images in χ, $\mathcal{C}_i$ and $\mathcal{C}$. It follows that Q_∞ is also the only ramified point of χ over $\mathcal{C}$. Note that $\chi \to \mathcal{C}$ is a Galois map since the Klein subgroup is normal in A_4. One can now see that the only possibility for the ramification structure over the point Q on $\mathcal{C}$ is the one in the following picture (see Abhyankar's lemma; i.e., Proposition III.8.9 in [14]).



This picture above means that Q has two points $\tilde{P}$ and P on the curve $\mathcal{C}_i$ ($i = 0$ or $i = 1$) above it and the ramification index of $\tilde{P}$ is $e(\tilde{P}|Q) = 3$. If $d(R|S)$ denotes the different of the point R over the point S, we then get

$$d(P_\infty|P) = d(Q_\infty|Q).$$

We now consider again the two subcases:

Subcase 2.1. The index 3 curve is isomorphic to $\mathcal{C}_0$ (see Equation (3.2)).

In this case we have (Hurwitz formula for $\mathcal{H} \to \mathcal{C}_0$)

$$d(Q_\infty|Q) = d(P_\infty|P) = 58.$$

It then follows that $g(\chi) = 99$ (Hurwitz formula for $\chi \to \mathcal{C}$).

Applying Hurwitz formula for the covering $\mathcal{H} \to \chi$ we get

$$700 = 2g(\mathcal{H}) - 2 \geq 4 \cdot (2 \times 99 - 2) = 784,$$

which is impossible.

Subcase 2.2. The index 3 curve is isomorphic to $\mathcal{C}_1$ (see Equation (3.3)).

In this case we have (as in Subcase 2.1)

$$d(Q_\infty|Q) = d(P_\infty|P) = 4 \quad \text{and} \quad g(\chi) = 72.$$

Looking at the covering $\mathcal{H} \xrightarrow{4} \chi$ of degree 4 and noticing that

$$\#\mathcal{H}(\mathbb{F}_{27^2}) = 1 + 27^3 = 19.684 \text{ rational points},$$

$$\#\chi(\mathbb{F}_{27^2}) = 1 + 27^2 + 2 \times 72 \times 27 = 4.618 \text{ rational points}$$

and moreover that $4 \times 4.618 = 18.472 < 19.684$, we can also discard this subcase.

We have then proved:

Proposition 1. *Suppose that a maximal curve $\mathcal{C}$ over $\mathbb{F}_{q^2}$ with $q = 27$, has genus 24 and that it is a Galois subcover of the Hermitian curve $\mathcal{H}$. Then this curve $\mathcal{C}$ is isomorphic to the curve given by the equation*

$$Y^9 - Y^3 + Y = X^7 \quad \textit{over} \quad \mathbb{F}_{27^2}.$$

Moreover the degree of the Galois covering $\varphi\colon \mathcal{H} \to \mathcal{C}$ satisfies $\deg\varphi = 12$.

Proof. The only possibility occurs in Subcase 1.1 of the Case $d = 12$ above.□

We can now state our main result:

Theorem 3. *Let $\mathcal{C}_3$ denote the $\mathbb{F}_{q^2}$-maximal curve where $q = 27$, with genus 24, which is given by the equation*

$$Y^9 - Y = X^7 \quad \textit{over} \quad \mathbb{F}_{27^2}.$$

Then the curve $\mathcal{C}_3$ is not a Galois subcover of the Hermitian curve $\mathcal{H}$.

Proof. From Proposition 1 we just have to prove that the following curves over $K = \mathbb{F}_{q^2}$ with $q = 27$, which are given by the equations:

$$\mathcal{C} := (Y^9 - Y^3 + Y = X^7) \quad \text{and} \quad \mathcal{C}_3 := (y^9 - y = x^7)$$

are not isomorphic to each other. Let P_∞ be the point at infinity on the first curve and Q_∞ be the point at infinity on the second curve. If we have an isomorphism $\sigma\colon \mathcal{C} \to \mathcal{C}_3$ we must have that $\sigma(P_\infty) = Q_\infty$ because these points are the only ones with Weierstrass semigroup $\langle 7, 9\rangle$ generated by the pole-orders 7 and 9 (see Satz 6 in [15]).

Since we have the following pole-divisors

$$\operatorname{div}_\infty(X) = 9P_\infty\ , \quad \operatorname{div}_\infty(Y) = 7P_\infty$$

and

$$\operatorname{div}_\infty(x) = 9Q_\infty\ , \quad \operatorname{div}_\infty(y) = 7Q_\infty$$

we must have nonzero constants a and c such that

$$\sigma(y) = aY + b \quad \text{and} \quad \sigma(x) = cX + dY + e.$$

Since $y^9 - y - x^7 = 0$ we get

$$(aY + b)^9 - (aY + b) - (cX + dY + e)^7 = 0.$$

The equation above should be a constant multiple of the equation

$$Y^9 - Y^3 + Y - X^7 = 0,$$

and this is impossible. □

Remark 4. Consider the maximal curves $\mathcal{C}_\ell$ over $\mathbb{F}_{q^2}$ with $q = \ell^3$ as in Theorem 1. We know that:

For $\ell = 2$, it is Galois covered by the Hermitian.
For $\ell = 3$, it is not Galois covered by the Hermitian.

- What is the situation for other values of ℓ ?
- Is the curve $\mathcal{C}_3$ covered by the Hermitian ?

References

[1] M. Abdón and A. Garcia. *On a characterization of certain maximal curves*. Finite Fields Appl. **10** (2004), 133–158.

[2] M. Abdón and F. Torres. *On maximal curves in characteristic two*. Manuscripta Math. **99** (1999), 39–53.

[3] A. Cossidente, G. Korchmáros and F. Torres. *On curves covered by the Hermitian curve*. J. Algebra **216** (1999), 56–76.

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

[5] R. Fuhrmann, A. Garcia and F. Torres. *On maximal curves*. J. Number Theory **67** (1997), 29–51.

[6] A. Garcia, H. Stichtenoth and C.P. Xing. *On Subfields of the Hermitian Function Field*. Compositio Math. **120** (2000), 137–170.

[7] A. Garcia and F. Torres. *On unramified coverings of maximal curves*, preprint (2005).

[8] Y. Ihara. *Some remarks on the number of rational points of algebraic curves over finite fields*. J. Fac. Sci. Tokio **28** (1981), 721–724.

[9] G. Korchmáros and F. Torres. *Embedding of a maximal curve in a Hermitian variety*. Compositio Math. **128** (2001), 95–113.

[10] G. Lachaud. *Sommes d'Eisenstein et Nombre de points de certaines courbes algébriques sur les corps finis*. C.R. Acad. Sci. Paris **305**, Serie I (1987), 729–732.

[11] M. Rosen. *The Hilbert class field in function fields*. Expo. Math. **5** (1987), 365–378.

[12] H.G. Rück and H. Stichtenoth. *A Characterization of Hermitian Function Fields over Finite Fields*. J. Reine Angew. Math. **457** (1994), 185–188.

[13] J.-P. Serre. *Algebraic groups and class fields*. Graduate Texts in Math. **117**, Springer, New York, 1988.

[14] H. Stichtenoth. *Algebraic Function Fields and Codes*, Springer, Berlin, 1993.

[15] H. Stichtenoth. *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik I, II*. Archiv der Math. **24** (1973), 524–544 and 615–631.

[16] K.O. Stöhr and J.F. Voloch. *Weierstrass points and curves over finite fields*. Proc. London Math. Soc. **52** (1986), 1–19.

[17] M. Tsfasman and S. Vladut. *Algebraic – Geometric Codes*, Kluwer, Dordrecht, 1991.

Arnaldo Garcia
IMPA – Estrada Dona Castorina 110
22460-320 – Rio de Janeiro
BRAZIL

E-mail: garcia@impa.br

Henning Stichtenoth
Universität Duisburg – Essen
Campus Essen, FB Mathematik
45117 Essen
GERMANY

E-mail: stichtenoth@ uni-essen.de

and

Sabanci University
MDBF, Orhanli
34956 Tuzla/Istanbul
TURKEY

E-mail: henning@ sabanciuniv.edu