On unramified coverings of maximal curves

Arnaldo Garcia* and Fernando Torres*

Abstract. We investigate unramified coverings of algebraic curves over a finite field, specially in relation with maximal curves and the question whether maximal curves are covered by the Hermitian curve.

1. Introduction

Let K denote the finite field with q^2 elements. An algebraic curve χ defined over K is said to be maximal if the cardinality of the set of K-rational points $\chi(K)$ attains the Hasse-Weil upper bound; i.e., if we have

$$\#\chi(K) = 1 + q^2 + 2q \cdot g(\chi),$$

where $g(\chi)$ denotes the genus of the curve.

From maximal curves one can construct interesting linear codes over finite fields. This construction of codes from algebraic curves is due to Goppa (see [7], [14] and [17]). Maximal curves have also very interesting properties with respect to their Jacobian varieties, their automorphism groups and also with respect to the Stöhr-Voloch theory on Frobenius-orders (see for example [12], [15], [18] and [16]).

Let $\varphi\colon \mathcal{Y} \to \chi$ be a surjective morphism of algebraic curves, where both curves χ and $\mathcal{Y}$ and also the map φ are all defined over K. In this situation we say that the curve χ is K-covered by the curve $\mathcal{Y}$. If the curve $\mathcal{Y}$ is maximal, then the curve χ is also a maximal curve over K. This result is due to Serre (see [10]).

The most interesting maximal curve over $K = \mathbb{F}_{q^2}$ is the so-called Hermitian curve (denoted by $\mathcal{H}$). This is the curve $\mathcal{H}$ given by the following plane equation:

$$X^{q+1} + Y^{q+1} + Z^{q+1} = 0.$$

The genus of the Hermitian curve satisfies

$$g(\mathcal{H}) = q(q-1)/2.$$

[0]* Both authors were partially supported by CNPq-Brazil (470193/03-4) and PRONEX (66.2408/96-9).

Ihara (see [8]) showed that if a curve χ is K-maximal then

$$g(\chi) \leq q(q-1)/2.$$

Rück-Stichtenoth (see [12]) showed that if a curve χ is K-maximal and its genus satisfies $g(\chi) = q(q-1)/2$ then χ is isomorphic to the Hermitian curve $\mathcal{H}$. We refer to [4], [3], [1] and [6] for other results on the classification of maximal curves with respect to their genera.

Many examples of maximal curves over K are obtained by considering quotient curves $\mathcal{H}/H$, where H is a subgroup of the automorphism group G of the Hermitian curve. This group G is huge (see [15]) and its order satisfies

$$|G| = q^3(q^3+1)(q^2-1).$$

For the construction of subcovers of the Hermitian curve via such subgroups of automorphisms H we refer to [6], [5] and [4].

The answer (yes or no) to the following question is unknown:

Question 1. *Are there maximal curves χ over K which are not K-covered by the Hermitian curve $\mathcal{H}$?*

The following theorem can be obtained from [12], [5], [9] and [2]:

Theorem 1. *Let $\mathcal{Y}$ be a maximal curve over $K = \mathbb{F}_{q^2}$ with genus $g(\mathcal{Y})$ satisfying*

$$6 \cdot g(\mathcal{Y}) > q^2 - q + 4.$$

Then the curve $\mathcal{Y}$ is K-covered by the Hermitian curve.

In this paper we will consider unramified K-coverings $\varphi\colon \mathcal{Y} \to \chi$, specially when the curve χ is maximal over K. In some cases we get that the curve $\mathcal{Y}$ is also K-maximal (see Proposition 1) and if the genus $g(\mathcal{Y})$ is very big (see Theorem 1) or the curve $\mathcal{Y}$ has a particular type of equation, one concludes that the curve χ is K-covered by the Hermitian.

We give examples of unramified coverings over $K = \mathbb{F}_{q^2}$ with both curves $\mathcal{Y}$ and χ maximal, and with $\mathcal{Y}$ being the curve associated to the Hilbert class field of the curve χ with respect to a certain subset S of rational points on it (see Example 1, Example 2 and Remark 3).

In Section 3 we introduce a certain maximal curve over $\mathbb{F}_{q^2}$ with $q = 8$ and we examine this maximal curve over $\mathbb{F}_{64}$ more closely in connection with unramified coverings and Question 1 (see Proposition 2). This certain maximal curve is the one given by the equation:

$$Y^4 + Y = X^3 \quad \text{over} \quad \mathbb{F}_{64}.$$

2. Unramified Coverings

By a curve χ over $K = \mathbb{F}_{q^2}$ we will always mean a projective, geometrically irreducible and nonsingular, algebraic curve defined over K. We denote by $\mathrm{Jac}(\chi)$ its Jacobian variety and we embed the curve χ in $\mathrm{Jac}(\chi)$ via the natural map:

$$P \in \chi \mapsto \mathrm{class}(P - P_0) \in \mathrm{Jac}(\chi),$$

where P_0 is a K-rational point on χ.

Let now χ be a K-maximal curve. Since the K-Frobenius morphism acts on $\mathrm{Jac}(\chi)$ as multiplication by $-q$ (see [12]) we get that the cardinality of the set $J(K)$ of K-rational points on $\mathrm{Jac}(\chi)$ satisfies

$$\#J(K) = (q+1)^{2\cdot g(\chi)}.$$

Let S be a subset of K-rational points of a curve χ over K (not necessarily a maximal curve); i.e., we have $S \subseteq \chi(K)$. We then denote by G_S the subgroup of $\mathrm{Jac}(\chi)$ generated by the points of S and by d_S the index

$$d_S := (J(K) \,:\, G_S).$$

Then there exists an unramified abelian K-covering of degree d_S (see [11] and [13])

$$\varphi_S \colon \chi_S \to \chi$$

such that the points of the set S splits completely under the map φ_S. The curve χ_S above corresponds to the Hilbert class field of the curve χ with respect to the set S.

We start with a proposition:

Proposition 1. *Let χ be a curve defined over $K = \mathbb{F}_{q^2}$ of genus g and let*

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

be an unramified K-covering of degree d.

Suppose that a set S of K-rational points on the curve χ splits completely under the map φ and that the cardinality of S satisfies

$$d \cdot (\#S) \geq (q+1)^2 + q \cdot d \cdot (2g-2).$$

Then both curves χ and $\mathcal{Y}$ are K-maximal.

Proof. Since φ is unramified we get

$$2g(\mathcal{Y}) - 2 = d \cdot (2g-2).$$

From the hypothesis that the set S is splitting completely we get

$$\#\mathcal{Y}(K) \geq d \cdot (\#S) \geq (q+1)^2 + q \cdot (2g(\mathcal{Y}) - 2).$$

From the Hasse-Weil upper bound for the curve $\mathcal{Y}$ we then see that

$$\#\mathcal{Y}(K) = (q+1)^2 + q \cdot (2g(\mathcal{Y}) - 2).$$

This means that the curve $\mathcal{Y}$ is K-maximal and a fortiori, the curve χ is also a K-maximal curve. □

Remark 1. With the hypothesis and notations of Proposition 1, suppose further that

$$d \cdot (q-1) + 1 > \frac{q^2 - q + 4}{6}.$$

It then follows from Theorem 1 that the curve $\mathcal{Y}$ (and a fortiori also the curve χ) is K-covered by the Hermitian curve $\mathcal{H}$.

Remark 2. The situation of a Hilbert class field of a curve χ over K with respect to an appropriate set S of K-rational points is the natural one to try to apply Proposition 1 and Remark 1 above. Voloch [18] describes a nice way to construct the corresponding covering curve χ_S and he proves that:

if $S = \chi(K)$ and $g(\chi) \leq (q+2)/8$, then $d_S = 1$.

Here on the contrary we are interested on the selection of an appropriate set of rational points S on a maximal curve χ leading to an unramified covering with degree $d > 1$.

Example 1. Let $n \in \mathbb{N}$, $n \geq 2$ and suppose that the characteristic p of K does not divide

$$d := n^2 - n + 1.$$

Suppose that d is a divisor of $q+1$ and consider the curve χ over $K = \mathbb{F}_{q^2}$ defined by the equation

$$X^n Y + Y^n Z + X Z^n = 0.$$

It is already known that χ is maximal over K and that it is K-covered by the Hermitian. Indeed denoting by $\mathcal{Y}$ the curve given by

$$u^d + v^d + w^d = 0,$$

we see that $\mathcal{Y}$ is covered by the Hermitian (since d is a divisor of $q+1$) and we have the following unramified covering

$$\begin{aligned} \varphi \colon \mathcal{Y} &\longrightarrow \chi \\ (u:v:w) &\longmapsto (u^n w : uv^n : vw^n). \end{aligned}$$

Let $P = (\alpha, \beta)$ with $\alpha \in K^*$ and $\beta \in K^*$ be an affine point on the curve χ; i.e., we have that

$$\alpha^{n-1} \cdot \beta + \alpha^{-1} \cdot \beta^n + 1 = 0.$$

Set $\gamma = \alpha^{n-1} \cdot \beta$, $\delta = \alpha^{-1} \cdot \beta^n$ and $m = (q+1)/d$, and consider the following set of rational points S on the curve χ

$$S = \{(\alpha, \beta) \in \chi \ ; \ \gamma^m \in \mathbb{F}_q \text{ and } \delta^m \in \mathbb{F}_q\} \cup \{P_1, P_2, P_3\},$$

where $P_1 = (1 : 0 : 0)$, $P_2 = (0 : 1 : 0)$ and $P_3 = (0 : 0 : 1)$. The set S splits completely under φ and after some computations we see that

$$\#S \geq \frac{(q+1)^2}{d} + q(d-3).$$

Noticing that we have

$$2g(\chi) - 2 = d - 3,$$

we can also deduce from Proposition 1 that the curve χ is K-maximal. This example illustrates that sometimes from the completely splitting of a small set of K-rational points (the set S is a small subset of $\chi(K)$ if the degree d is big) one can deduce the maximality of the curve.

Remark 3. With notation as in Example 1 we have determined the Hilbert class field, since

$$\chi_S = \mathcal{Y} \text{ and hence } d_S = d.$$

Indeed we have

$$\chi_S \xrightarrow{d'} \mathcal{Y} \xrightarrow{d} \chi$$

where d' denotes the degree of χ_S over $\mathcal{Y}$. We also have

$$2g(\chi_S) - 2 = d' \cdot (2g(\mathcal{Y}) - 2)$$

and moreover since all points of $\mathcal{Y}(K)$ should split completely in χ_S we get

$$(q+1)^2 + q(2g(\chi_S) - 2) \geq d' \cdot \big((q+1)^2 + q(2g(\mathcal{Y}) - 2)\big).$$

From this it follows that $d' = 1$.

Example 2. Consider the curve χ over K with the affine plane equation

$$Y^{q+1} + X^{(q+1)/d} + X^{2(q+1)/d} = 0,$$

where d is an odd divisor of $q+1$. The genus of χ satisfies

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

The Hermitian curve $\mathcal{H}$ (given by $u^{q+1} + v^{q+1} + 1 = 0$) covers the curve χ via the unramified morphism of degree d below

$$\varphi \colon \mathcal{H} \longrightarrow \chi$$
$$(u : v : 1) \longmapsto (u^d : uv : 1).$$

Let $P = (\alpha, \beta)$ be a K-rational point on the curve χ; i.e.,

$$\beta^{q+1} + \alpha^{(q+1)/d} + \alpha^{2(q+1)/d} = 0.$$

Set now $\gamma = \alpha^{(q+1)/d}$ and $\delta = \gamma + \gamma^2$, and consider the set S of rational points on χ given by $S = \chi(K) \setminus W$ with $W = \{P \ ; \ \gamma \notin \mathbb{F}_q \text{ and } \delta \in \mathbb{F}_q\}$. One can see that S splits completely under the morphism φ above and moreover, as in Remark 3, that the Hermitian curve corresponds to the Hilbert class field of χ with respect to this set S. □

3. A certain maximal curve

In his lecture at the conference AGCT-10, J.-P. Serre pointed out that the following equation

$$Y^4 + Y = X^3$$

defines a maximal curve χ over $\mathbb{F}_{64}$ with genus 3. The Hermitian curve $\mathcal{H}$ over $\mathbb{F}_{64}$ can be given by the following equation

$$Z^8 + Z = W^9.$$

Performing the substitutions $x = W^3$ and $y = Z^2 + Z$, one sees that the curve χ_1 given by

$$y^4 + y^2 + y = x^3$$

is K-covered by the Hermitian curve $\mathcal{H}$ and hence the curve χ_1 is maximal over $\mathbb{F}_{64}$ with genus 3. However one can show that the curves χ and χ_1 are not isomorphic.

This raises the question (see Question 1): *Is the curve χ given by the equation $Y^4 + Y = X^3$ over $\mathbb{F}_{64}$ a subcover of the Hermitian curve*?

We will prove that χ is a Galois subcover of $\mathcal{H}$ with degree $= 9$. We will show that we have an intermediate curve $\mathcal{Y}$ and two maps ψ and φ (both of degree 3)

$$\mathcal{H} \xrightarrow{\psi} \mathcal{Y} \xrightarrow{\varphi} \chi$$

with the above map φ unramified. We also show that the Hermitian curve is a Galois cover of χ with a Galois group isomorphic to $\dfrac{\mathbb{Z}}{3\mathbb{Z}} \times \dfrac{\mathbb{Z}}{3\mathbb{Z}}$.

Consider the curve $\mathcal{Y}$ over $\mathbb{F}_{64}$ given by

$$Z^8 + Z = x^3.$$

Of course the substitution $x = W^3$ gives the map ψ from $\mathcal{H}$ to the curve $\mathcal{Y}$ above. We can now state our result:

Proposition 2. *The curve $\mathcal{Y}$ above has an automorphism σ of order 3 and without fixed points, such that the quotient curve $\mathcal{Y}/\langle\sigma\rangle$ is isomorphic to the curve χ.*

Proof. Consider the following automorphism σ of the curve $\mathcal{Y}$ (see [15]):

$$\sigma(Z) = 1 + Z^{-1} \text{ and } \sigma(x) = \frac{ax}{Z^3} \text{ with } a^2 = a + 1.$$

One checks easily that σ is of order 3 and that it has no fixed points on the curve $\mathcal{Y}$. Consider the following functions on $\mathcal{Y}$ that are invariant under the automorphism σ (hence they are functions on the quotient curve):

$$w = \frac{Z^3 + Z + 1}{Z^2 + Z} \quad \text{and} \quad t = x + \sigma(x) + \sigma^2(x).$$

After long computations one sees that the following holds:

$$t^3 = (w^4 + w)(w + a)^4 \quad \text{with} \quad a^2 = a + 1 \quad \text{as above.}$$

The equation above is then an equation for the quotient curve $\mathcal{Y}/\langle\sigma\rangle$. Using that $a^4 = a$ and setting

$$X = t \cdot (w + a)^{-3} \quad \text{and} \quad Y = (w + a)^{-1},$$

we get the desired relation

$$Y^4 + Y = X^3.$$

□

Acknowledgements. We are thankful to Rainer Fuhrmann and to Henning Stichtenoth for several discussions on the subject of this paper.

References

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

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

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

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

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

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

[7] V.D. Goppa – *Geometry and Codes*, in: Mathematics and its Applications, vol **24**. Kluwer Academic Publisher, Dordrechet – Boston – London, 1988.

[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, F. Torres – *On the genus of a maximal curve*. Math Annalen **323** (2002), 589–608.

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

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

[18] J.F. Voloch – *Jacobians of curves over finite fields*. Rocky Mountain J. Math. **30**, 755–759, (2000).

Addresses:

Arnaldo Garcia
IMPA - Estrada Dona Castorina 110
22.460-320 - Rio de Janeiro - Brazil
e-mail: garcia@impa.br

Fernando Torres
UNICAMP - Instituto de Matemática
Caixa Postal 6065
13.083-970 - Campinas - Brazil
e-mail: ftorres@ime.unicamp.br