A remark on maximal curves and unramified coverings

Rainer Fuhrmann[a], Arnaldo Garcia[b,(⋆)] and Fernando Torres[c,(⋆)]

[a] *IBM, Unternehmensberatung, D-40474, Düsseldorf, Germany*

[b] *IMPA, 22460-320, Rio de Janeiro, Brazil*

[c] *IMECC-UNICAMP, 13083-970, Campinas, Brazil*

Abstract

We give a sufficient condition for a given maximal curve to be covered by another maximal curve, with the covering being unramified. We also provide examples illustrating this phenomena.

Key words: maximal curves, abelian unramified coverings.

MSC: 11G20, 14G05, 14G15

1 Introduction

Let χ be a projective, geometrically irreducible, nonsingular algebraic curve defined over the finite field $\mathbb{F}_{q^2}$ with q^2 elements. A celebrated theorem of A. Weil (see [10] and [8]) says that the set $\chi(\mathbb{F}_{q^2})$ of rational points on the curve

⋆ The second and third authors acknowledge the partial support from CNPq/PRONEX # 66.2408/1996-3.

χ over $\mathbb{F}_{q^2}$ satisfies

$$\#\ \chi(\mathbb{F}_{q^2}) \leq (q+1)^2 + q(2g-2), \qquad \text{where } g \text{ denotes the genus of } \chi.$$

The curve χ is said to be $\mathbb{F}_{q^2}$-*maximal* if it attains the bound above; i.e.,

$$\#\,\chi(\mathbb{F}_{q^2}) = (q+1)^2 + q \cdot (2g-2).$$

It is a result of Ihara (see [4]) that the genus of a maximal curve satisfies:

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

There is a unique $\mathbb{F}_{q^2}$-maximal curve having genus $g = q(q-1)/2$ (see [6]). This is the so-called *Hermitian curve* over $\mathbb{F}_{q^2}$ and it can be given in the projective plane by the equation:

$$U^{q+1} + V^{q+1} + W^{q+1} = 0.$$

It is a result of J.-P. Serre (see [5, Prop. 6]) that if a curve χ is $\mathbb{F}_{q^2}$-covered by a maximal curve $\mathcal{C}$ over $\mathbb{F}_{q^2}$, then the curve χ is also $\mathbb{F}_{q^2}$-maximal; i.e., if we have a surjective morphism (defined over $\mathbb{F}_{q^2}$) $\mathcal{C} \twoheadrightarrow \chi$ and if $\mathcal{C}$ is $\mathbb{F}_{q^2}$-maximal, then the curve χ is also $\mathbb{F}_{q^2}$-maximal. Here on the contrary we start with a $\mathbb{F}_{q^2}$-maximal curve χ and we look for sufficient conditions so that we get a surjective unramified morphism (defined over $\mathbb{F}_{q^2}$)

$$\mathcal{C} \twoheadrightarrow \chi$$

with the curve $\mathcal{C}$ above also $\mathbb{F}_{q^2}$-maximal.

2 The Remark

Let us denote by $\mathcal{J}$ the Jacobian variety of the curve χ and by $\mathcal{J}(\mathbb{F}_{q^2})$ its set of $\mathbb{F}_{q^2}$-rational points. Fixing a rational point P_0 over $\mathbb{F}_{q^2}$ on the curve χ, we embedd the curve in the Jacobian by the map φ below:

$$\begin{aligned} \chi &\xrightarrow{\varphi} \mathcal{J} \\ P &\longmapsto \text{class}(P - P_0). \end{aligned}$$

Let $S \subseteq \chi(\mathbb{F}_{q^2})$ be a subset of $\mathbb{F}_{q^2}$-rational points on χ and we denote by G_S the subgroup of $\mathcal{J}(\mathbb{F}_{q^2})$ generated by $\varphi(P)$ as the point P runs thru the elements of S; i.e.,

$$G_S = \langle \varphi(P) \mid P \in S \rangle \subseteq \mathcal{J}(\mathbb{F}_{q^2}).$$

We know that $\#\mathcal{J}(\mathbb{F}_{q^2}) = (q+1)^{2g}$, where g is the genus of the $\mathbb{F}_{q^2}$-maximal curve χ (see [6, Lemma 1]). A fundamental object of study in Class Field Theory of algebraic curves is the maximal unramified abelian $\mathbb{F}_{q^2}$-covering of the curve χ in which every point of the subset S splits completely (see [7]). Let us denote this unramified covering by

$$\pi_S : \chi_S \twoheadrightarrow \chi.$$

We have the following

$$d_S := \deg \pi_S = (\mathcal{J}(\mathbb{F}_{q^2}) : G_S),$$

where the index is the cardinality of the quotient group; i.e.,

$$(\mathcal{J}(\mathbb{F}_{q^2}) : G_S) = \#(\mathcal{J}(\mathbb{F}_{q^2})/G_S).$$

We can now state our main remark.

Remark 1. *Let χ be a $\mathbb{F}_{q^2}$-maximal curve with genus g and let S be a subset of $\chi(\mathbb{F}_{q^2})$. Suppose that $d_S = \text{degree}(\pi_S)$ satisfies the following two conditions:*

i) d_S is a divisor of $(q+1)^2$.

ii) $\#S = (q+1)^2 + q(2g-2) - a$, with $d_S \cdot a = (q+1)^2 \cdot (d_S - 1)$.

Then the maximal unramified abelian covering χ_S (as above) is also a $\mathbb{F}_{q^2}$-maximal curve.

Proof: From Hurwitz's formula we have

$$2g_S - 2 = d_S \cdot (2g-2), \qquad \text{where } g_S \text{ denotes the genus of } \chi_S.$$

We also have

$$\#\chi_S(\mathbb{F}_{q^2}) \geq d_S \cdot (\#S),$$

since the points in S split completely. The hypothesis (conditions i) and ii) above) gives

$$d_S \cdot (\#S) = (q+1)^2 + q(2g_S - 2).$$

On the other hand by A. Weil's theorem we always have:

$$\#\chi_S(\mathbb{F}_{q^2}) \leq (q+1)^2 + q(2g_S - 2).$$

This shows that the curve χ_S is also $\mathbb{F}_{q^2}$-maximal. $\square$

Remark 2. The number a in condition ii) of Remark 1 is just

$$a = \#(\chi(\mathbb{F}_{q^2}) \setminus S).$$

Recently J.F. Voloch (see [9]) describes a very nice way to construct the curves χ_S and it was this paper that triggered our interest here.

The hard thing here is to find a maximal curve χ and a subset $S \subseteq \chi(\mathbb{F}_{q^2})$ satisfying conditions i) and ii) of Remark 1. This is the content of the next section.

3 Examples for Remark 1

We are now going to give two examples illustrating the phenomena in Remark 1. We are going to omit essentially all the details of proofs.

Example 1. Consider the curve χ over $\mathbb{F}_{q^2}$ given by the following affine equation

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

where d is an odd divisor of $(q+1)$.

One can view this curve χ as a degree $(q+1)$ Kummer cover of the projective x-line and using the results in [3] one computes the genus $g := g(\chi)$ as

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

The curve χ is indeed $\mathbb{F}_{q^2}$-maximal and to prove it one has to show that

$$\#\{\alpha \in \mathbb{F}_{q^2} \mid \alpha^{(q+1)/d} + \alpha^{2(q+1)/d} \in \mathbb{F}_q^*\} = (q+1) + (q+1)(q-3)/d.$$

To establish the equality above we consider

$$\begin{aligned} \mathbb{F}_{q^2}^* &\longrightarrow \mathbb{F}_{q^2}^* \\ \alpha &\longmapsto w := \alpha^{(q+1)/d} \end{aligned}$$

and we have to check the following equality

$$\#W_1 = (d-1) \text{ with } W_1 := \{w \in \mathbb{F}_{q^2} \setminus \mathbb{F}_q;\ w^{d(q-1)} = 1 \text{ and } w^2 + w \in \mathbb{F}_q\}.$$

It follows from the equality above that

$$\#W = (q+1)^2(d-1)/d,$$

where W is the subset of $\chi(\mathbb{F}_{q^2})$ below

$$W := \{(x,y) \in \chi\ ;\ x^{(q+1)/d} \in W_1\}.$$

We now consider

$$S := \chi(\mathbb{F}_{q^2}) \setminus W.$$

To finish the proof that the curve χ here illustrates Remark 1, one has the difficult task of showing the claim:

Claim. $(\mathcal{J}(\mathbb{F}_{q^2}) : G_S) = d.$

We are not going to give a direct proof of this claim. The maximal curve χ_S obtained thru Remark 1 satisfies

$$g(\chi_S) = q(q-1)/2,$$

and hence it is the Hermitian curve (see [6]). The result in [2, Example 5.10] gives an indirect proof of the Claim above.

Example 2. Let $n \in \mathbb{N}$, $n \geq 2$, be such that

$$d := (n^2 - n + 1) \quad \text{is a divisor of} \quad (q+1).$$

Consider the Hurwitz curve χ given by

$$f(X, Y) = Y^n + X^n Y + X.$$

The Fermat curve $\mathcal{F}$ with exponent d; i.e., the curve $\mathcal{F}$ given by

$$F(U, V) = U^d + V^d + 1$$

is $\mathbb{F}_{q^2}$-maximal since d is a divisor of $(q+1)$. Hence the Hurwitz curve χ is also $\mathbb{F}_{q^2}$-maximal since it is covered by $\mathcal{F}$; in fact, we have the following map

$$\begin{aligned} \pi \colon \mathcal{F} &\longrightarrow \chi \\ (u, v) &\longmapsto (u^n/v, uv^{n-1}). \end{aligned}$$

One can check that $\deg \pi = d$, the map π is unramified and moreover that each point of S splits completely under π, where the set S is the subset of $\chi(\mathbb{F}_{q^2})$ given by:

$$S := \{(x, y) \in \chi(\mathbb{F}_{q^2});\ x \neq 0 \text{ and } (yx^{n-1})^{\frac{q+1}{d}}, (x^{-1}y^n)^{\frac{q+1}{d}} \in \mathbb{F}_q\} \cup \{P_1, P_2, P_3\},$$

where $P_1 = (1 : 0 : 0)$, $P_2 = (0 : 1 : 0)$ and $P_3 = (0 : 0 : 1)$. Also, after some computations one sees that

$$\#S = (q+1)^2/d + q(d-3).$$

To finish the proof that the Hurwitz curve χ illustrates Remark 1, one has the difficult task of showing the claim:

Claim. $(\mathcal{J}(\mathbb{F}_{q^2}) : G_S) = d$.

We are not going to give the proof of this claim here. We notice that in the particular case when $n = 2$ (and assuming that $d = 3$ is a divisor of $(q+1)$), the Hurwitz curve χ is an elliptic curve and one can check that the set S is a group in this case (i.e., $G_S = S$). This can be proved using the explicit formulas for the group law on the elliptic curve χ. We omit the details. From above we conclude that the curve χ_S in Remark 1 satisfies $\chi_S = \mathcal{F}$.

References

[1] A. Aguglia, G. Korchmáros and F. Torres, Plane maximal curves, to appear in Acta Arithmetica.

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

[3] H. Hasse, Theorie der relativ zyklischen algebraischen Funktionenkörper, *J. Reine Angew. Math.* **172** (1934), 37–54.

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

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

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

[7] J.P. Serre, Algebraic Groups and Class Fields (GTM **117**, Springer-Verlag, New York, 1988).

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

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

[10] A. Weil, Courbes algébriques et variétés abéliennes (Hermann, Paris, 1971).