ON MAXIMAL CURVES AND UNRAMIFIED COVERINGS

RAINER FUHRMANN, ARNALDO GARCIA, AND FERNANDO TORRES

Abstract. We discuss sufficient conditions for a given curve to be covered by a maximal curve with the covering being unramified; it turns out that the given curve itself will be also maximal. We relate our main result to the question of whether or not a maximal curve is covered by the Hermitian curve. We also provide examples illustrating the results.

§1. Let $\mathcal{X}$ be a projective, geometrically irreducible, non-singular algebraic curve of genus g defined over the finite field $\mathbf{F}_{q^2}$ with q^2 elements, and let $\mathcal{J}$ be the Jacobian variety of $\mathcal{X}$. A celebrated theorem of A. Weil gives in particular the following upper bound for the cardinality of the set $\mathcal{X}(\mathbf{F}_{q^2})$ of $\mathbf{F}_{q^2}$-rational points on the curve:

$$\#\mathcal{X}(\mathbf{F}_{q^2}) \le (q+1)^2 + q(2g-2)\,.$$

The curve $\mathcal{X}$ is called $\mathbf{F}_{q^2}$*-maximal* if it attains the upper bound above; i.e., if one has

$$\#\mathcal{X}(\mathbf{F}_{q^2}) = (q+1)^2 + q(2g-2)\,.$$

Equivalently, the curve $\mathcal{X}$ is $\mathbf{F}_{q^2}$-maximal if the $\mathbf{F}_{q^2}$-Frobenius endomorphism on the Jacobian $\mathcal{J}$ acts as a multiplication by $-q$; see [13], [6, Lemma 1.1].

The most well-known example of a $\mathbf{F}_{q^2}$-maximal curve is the so-called *Hermitian curve* $\mathcal{H}$, which can be given by the plane model

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

By a result of Serre, see [10, Prop. 6], every curve $\mathbf{F}_{q^2}$-covered by a $\mathbf{F}_{q^2}$-maximal curve is also $\mathbf{F}_{q^2}$-maximal. Thus many examples of $\mathbf{F}_{q^2}$-maximal curves arise by considering quotient curves $\mathcal{H}/G$, where G is a subgroup of the automorphism group of $\mathcal{H}$; see [7], [4], [5]. Serre's result points out the following.

Question. Is any $\mathbf{F}_{q^2}$-maximal curve $\mathbf{F}_{q^2}$-covered by the Hermitian curve $\mathcal{H}$?

So far, this question is an open problem but a positive answer is known whenever the genus is large enough:

Lemma. ([9, Thm. 3.1], [13], [6, Thm. 3.1], [1]) *A $\mathbf{F}_{q^2}$-maximal curve of genus larger than $\lfloor (q^2-q+4)/6 \rfloor$ is $\mathbf{F}_{q^2}$-covered by the Hermitian curve.*

2000 *Mathematics Subject Classification*: Primary 11G20; Secondary 14G05, 14G15.

Key words and phrases: finite field, maximal curve, Hilbert class field.

Garcia and Torres acknowledge partial support from Cnpq-Brazil and PRONEX 41.96.0883.00. The authors are indebted to J.F. Voloch for sending us his paper [18].

In this note we discuss sufficient conditions for a given curve to be $\mathbf{F}_{q^2}$-covered by a $\mathbf{F}_{q^2}$-maximal curve with the covering being unramified (see the Theorem below); a posteriori, the given curve itself will be $\mathbf{F}_{q^2}$-maximal by the aforementioned Serre's result. In particular, we obtain the Corollary after Remark 3, a result related to the Question in §1. The crucial technique here is Class Field Theory: see Remark 2.

§2. For a subset S of the set of $\mathbf{F}_{q^2}$-rational points of the curve $\mathcal{X}$, we denote by G_S the subgroup of $\mathcal{J}(\mathbf{F}_{q^2})$ generated by the points in S (as usually one embedds the curve in its Jacobian $\mathcal{J}$ by fixing one $\mathbf{F}_{q^2}$-rational point as the zero element of the group law of the Jacobian). We set

$$d_S := (\mathcal{J}(\mathbf{F}_{q^2}) : G_S)\,.$$

Remark 1. If $\mathcal{X}$ is $\mathbf{F}_{q^2}$-maximal, the set of $\mathbf{F}_{q^2}$-rational points of its Jacobian variety $\mathcal{J}$ coincide with its $(q+1)$-torsion points and so $\#\mathcal{J}(\mathbf{F}_{q^2}) = (q+1)^{2g}$; see [13, Lemma 1].

Remark 2. Let $\mathcal{X}$ and S be as above. The maximal unramified abelian $\mathbf{F}_{q^2}$-covering $\pi_S : \mathcal{X}_S \to \mathcal{X}$ of $\mathcal{X}$ in which every point of S splits completely is the fundamental object of study in Class Field Theory of curves; cf. [15, Ch. VI, Thm. 4], [12, Thm. 1.3]. We have that $\pi_S^{-1}(S) \subseteq \mathcal{X}_S(\mathbf{F}_{q^2})$, and that the covering degree of π_S is equal to d_S (loc. cit., or see below); in addition, $\mathcal{X}_S$ is the $\mathbf{F}_{q^2}$ non-singular model of the Hilbert class field of $\mathbf{F}_{q^2}(\mathcal{X})$ with respect to the set S (loc. cit.).

Recently, Voloch [18] describes a nice way to construct the curve $\mathcal{X}_S$. We briefly describe his construction here for completeness. Let $\alpha : \mathcal{J} \to \mathcal{J}$ be the surjective $\mathbf{F}_{q^2}$-endomorphism given by $x \mapsto x - \phi(x)$, with ϕ being the $\mathbf{F}_{q^2}$-Frobenius endomorphism on $\mathcal{J}$. We have an $\mathbf{F}_{q^2}$-isogeny $\psi : \mathcal{J}/G_S \to \mathcal{J}$, $\psi(\bar{x}) := \alpha(x)$, whose degree is d_S. Now let $\mathcal{X}'$ be the pull-back of $\mathcal{X}$ by ψ which clearly induces an unramified abelian $\mathbf{F}_{q^2}$-covering $\pi' : \mathcal{X}' \to \mathcal{X}$ of degree d_S. To see that S splits under π', let $\beta : \mathcal{J}/G_S \to \mathcal{J}/G_S$ be given by $\bar{x} \mapsto \overline{\alpha(x)}$. Then $G_S = \psi((\mathcal{J}/G_S)(\mathbf{F}_{q^2}))$ (loc. cit.), so that

$$S \subseteq G_S \subseteq \mathcal{X}' \cap (\mathcal{J}/G_S)(\mathbf{F}_{q^2}) = \mathcal{X}'(\mathbf{F}_{q^2})\,,$$

and hence that $\pi' = \pi_S$.

§3. Now we state the main result of this paper.

Theorem. *Let $\mathcal{X}$, S, and d_S be as above. Let $\pi_S : \mathcal{X}_S \to \mathcal{X}$ be the maximal unramified abelian $\mathbf{F}_{q^2}$-covering of $\mathcal{X}$ in which every point of S splits completely. Suppose that the following two conditions hold:*

(i) *d_S is a divisor of $(q+1)^2$,*
(ii) $\#S = (q+1)^2/d_S + q(2g-2)$.

Then both curves $\mathcal{X}_S$ and $\mathcal{X}$ are $\mathbf{F}_{q^2}$-maximal.

Proof. As was observed in Remark 2, the covering degree of π_S is d_S. Since π_S is unramified, from the Riemann-Hurwitz formula we have $2g'-2 = d_S(2g-2)$, where g' stands for the genus of the curve $\mathcal{X}_S$. Since the points in S split completely and by the assumption on $\#S$, we have

$$\#\mathcal{X}_S(\mathbf{F}_{q^2}) \geq d_S\cdot(\#S) = (1+q)^2 + q(2g'-2)\,.$$

Hence we must have that the inequality above is actually an equality, as follows from Weil's theorem and thus the curve $\mathcal{X}_S$ is $\mathbf{F}_{q^2}$-maximal. Finally, the curve $\mathcal{X}$ is also $\mathbf{F}_{q^2}$-maximal by Serre's result [10, Prop. 6]. □

Remark 3. In the Theorem, the morphism $\pi_S : \mathcal{X}_S \to \mathcal{X}$ can be replace by any unramified $\mathbf{F}_{q^2}$-covering $\pi' : \mathcal{X}' \to \mathcal{X}$ of covering degree d whenever ${\pi'}^{-1}(S) \subseteq \mathcal{X}'(\mathbf{F}_{q^2})$, and whenever d and $\#S$ satisfy the hypotheses in the theorem. Moreover, if such a morphism $\pi' : \mathcal{X}' \to \mathcal{X}$ is abelian, then $\pi' = \pi_S$. Indeed, we have ${\pi'}^{-1}(S) = \mathcal{X}'(\mathbf{F}_{q^2})$ and there is an unramified $\mathbf{F}_{q^2}$-covering $\mathcal{X}_S \to \mathcal{X}'$ of degree d' in which every point of $\mathcal{X}'(\mathbf{F}_{q^2})$ splits completely. Let g'' and g' be the genus of $\mathcal{X}_S$ and $\mathcal{X}'$ respectively. Then $2g''-2 = d'(2g'-2)$ and from

$$(q+1)^2 + q(2g''-2 \geq \#\mathcal{X}_S(\mathbf{F}_{q^2}) \geq d'\#\mathcal{X}'(\mathbf{F}_{q^2}) = d'(q+1)^2 + q(2g''-2)\,,$$

we see that $d' = 1$.

The following consequence of the Theorem improves on the Lemma in §1.

Corollary. *Suppose that the curve $\mathcal{X}$ is $\mathbf{F}_{q^2}$-maximal of genus g, and that d_S and S fulfill the hypotheses in the Theorem. In addition, suppose that*

$$g > 1 + (\lfloor (q^2-q+4)/6\rfloor - 1)/d_S\,.$$

Then the curve $\mathcal{X}$ is $\mathbf{F}_{q^2}$-covered by the Hermitian curve $\mathcal{H}$.

Proof. Let $\pi_S : \mathcal{X}_S \to \mathcal{X}$ be the maximal unramified abelian $\mathbf{F}_{q^2}$-covering of $\mathcal{X}$ in which any point of S splits completely. The genus g' of $\mathcal{X}_S$ satisfies $g' = d_S(g-1)+1$, so that we have $g' > \lfloor (q^2-q+4)/6\rfloor$ by the hypothesis on g. Therefore from the Theorem and the Lemma, the curve $\mathcal{X}_S$ is $\mathbf{F}_{q^2}$-covered by the Hermitian curve and hence the curve $\mathcal{X}$ is also. □

Remark 4. The Corollary improves on the Lemma if we can find a subset S of $\mathbf{F}_{q^2}$-rational points fulfilling the hypotheses in the Theorem and such that $d_S > 1$.

Voloch [18] showed that for a curve $\mathcal{Y}$ of genus $\tilde{g}$ over $\mathbf{F}_\ell$, and for $S = \mathcal{Y}(\mathbf{F}_\ell)$, the condition $\ell \geq (8\tilde{g}-2)^2$ implies that $d_S = 1$. (We observe that the condition just mentioned in the case of a $\mathbf{F}_{q^2}$-maximal curve of genus g, can only happen if $g \leq (q+2)/8$.) Voloch also constructed curves with many rational points by choosing properly the subset S. This technique was also explored by several authors to the construction of infinite class field towers aiming to good lower bounds on the asymptotic behaviour of the ratio of rational points by the genus; see e.g. [14], [16], [11].

In general, it is not an easy task the selection of the subset S of $\mathbf{F}_{q^2}$-rational points satisfying both, the hypotheses in the Theorem and the condition $d_S > 1$. In the next example we are going to see this in a very particular situation (see Remark 5 for the general case).

Example. Let $n \in \mathbf{N}$, $n \geq 2$, be such that $\mathrm{char}(\mathbf{F}_{q^2})$ does not divide $d := n^2 - n + 1$. We assume moreover that d is a divisor of $q+1$. We shall consider certain subset S of Hurwitz curves $\mathcal{H}_n$, which are the curves defined by

$$U^nV + V^nW + W^nU = 0\,.$$

We set

$$\begin{aligned} S :=&\{(u:v:1) : u, v \in \mathbf{F}^*_{q^2}; u^{n-1}v + u^{-1}v^n + 1 = 0 \text{ and } (u^{n-1}v)^{\frac{q+1}{d}}, (u^{-1}v^n)^{\frac{q+1}{d}} \in \mathbf{F}_q\} \cup \\ &\{P_1, P_2, P_3\}\,, \end{aligned}$$

where $P_1 := (1:0:0), P_2 := (0:1:0)$, and $P_3 := (0:0:1)$. Clearly the set S is contained in $\mathcal{H}_n(\mathbf{F}_{q^2})$. Notice that the genus g of the Hurwitz curve $\mathcal{H}_n$ satisfies $2g-2 = d-3$.

Claim 1. *For $n = 2$, and $q = 5$ or $q = 11$, we have $d = 3$ and*

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

To prove the claim above let us first explain some general facts. Let π be the plane morphism given by

$$(u:v:1) \mapsto (u^{n-1}v : u^{-1}v^n : 1)\,.$$

Then $\pi(\mathcal{H}_n)$ is the line $\mathcal{L} : X + Y + Z = 0$ in $\mathbf{P}^2(\bar{\mathbf{F}}_{q^2})$ and $\pi : \mathcal{H}_n \to \mathcal{L}$ is a d-sheeted covering which is (totally) ramified exactly at P_1, P_2, and P_3. (Notice that $\pi(P_1) = (-1 : 0 : 1), \pi(P_2) = (-1:1:0)$, and $\pi(P_3) = (0:-1:1)$.) Now each d-th root of unity belongs to $\mathbf{F}_{q^2}$ since d divides $q+1$ and so, for $u, v \in \mathbf{F}^*_{q^2}$,

$$\pi^{-1}(u^{n-1}v : u^{-1}v^n : 1) = \{(\eta^n u : \eta v : 1) : \eta^d = 1\} \subseteq \mathcal{H}_n(\mathbf{F}_{q^2})\,.$$

Therefore $(\#S - 3)/d = t := \#\{(x,y) \in \mathbf{F}^*_{q^2} \times \mathbf{F}^*_{q^2} : x + y + 1 = 0 \text{ and } x^{\frac{q+1}{d}}, y^{\frac{q+1}{d}} \in \mathbf{F}_q\}$. We have thus to show that

$$t = q + (q+1)^2/d^2 - 3(q+1)/d = (q+1)^2/d^2 - 1\,.$$

Now let $q = 5$ or $q = 11$. Then the quadratic polynomial $X^2 + X + 1$ is irreducible in $\mathbf{F}_q[X]$, and therefore the elements of $\mathbf{F}_{q^2}$ can be written as $a + b\alpha$ with $a, b \in \mathbf{F}_q$ and $\alpha^2 = -\alpha - 1$.

Case $n = 2, q = 5$. Here $(q+1)/d = 2$ and we have to show that $t = q-2$. We have to consider pairs $(x,y) \in \mathbf{F}^*_{q^2} \times \mathbf{F}^*_{q^2}$ with $x = a + b\alpha, y = c - b\alpha$, and $a + c = -1$. For a fixed pair (a,c), we have $x^2, y^2 \in \mathbf{F}_q$ if and only if $2ab - b^2 = 0$ and $2cb + b^2 = 0$. Both equations have a common root only if $b = 0$, so that $x = a$ and $y = c$ and therefore $t = q-2$, since we have to exclude the possibilities $a = 0$ and $a = -1$.

Case $n=2, q=11$. Here $(q+1)/d=4$ and we have to show that $t=q+4$. Notice that $\alpha^3=1$. Let $x=a+b\alpha$ and $y=c-b\alpha$, as in the previous case. For a given pair (a,c), $x^4, y^4 \in \mathbf{F}_q$ if and only if $4a^3b-6a^2b^2+b^4=0$ and $-4c^3b-6c^2b^2+b^4=0$. Arguing as in the previous case, $b=0$ provides with $q-2$ elements in $\pi(S\setminus\{P_1,P_2,P_3\})$. Now if $b\neq 0$ in a common solution of the above equations, then $b=8(a^2-ac+c^2)/(a-c)$ and the following possibilities arise:

$$\begin{aligned}(a,c,b)\in\{&(1,-2,4),(-2,1,-4),(2,-3,4),(-3,2,-4),(3,-4,3),(-4,3,-3),\\ &(4,-5,9),(-5,4,-9)\}\,.\end{aligned}$$

A straightforward computation shows that only the cases $(3,-4,3),(-4,3,-3)$ cannot occur; so that $t=(q-2)+6=q+4$. This finishes with Claim 1.

Claim 2. *Take $\mathcal{H}_n$ and S as in the Example. For $n=2$ and $\mathrm{char}(\mathbf{F}_{q^2})>2$ we have that $G_S=S$.*

The curve $\mathcal{H}_2$ is an elliptic curve and so we can use explicit formulas for the group law. To this end we look for a Weierstrass form of $\mathcal{H}_2$. Set

$$\varphi:(U:V:W)\mapsto(X:Y:Z):=(UW:2VW+U^2:U^2)\,.$$

Then it is easy to see that φ induces an $\mathbf{F}_{q^2}$-isomorphism between $\mathcal{H}_2$ and the curve

$$\mathcal{X}:=\varphi(\mathcal{H}_2):Y^2Z=Z^3-4X^3\,.$$

We have that $\varphi(S)=T\cup\{P_1',P_2',P_3'\}$, where

$$T=\{(x:y:1):x,y\in\mathbf{F}_{q^2};y^2=1-4x^3;(y-1)^{(q+1)/3}\in\mathbf{F}_q\}$$

and $P_1'=\varphi((1:0:0))=(0:1:1)$, $P_2'=\varphi((0:1:0))=(0:-1:1)$, and $P_3'=\varphi((0:0:1))=(0:1:0)$.

Let $\oplus$ denote the group addition of the curve $\mathcal{X}$ with neutral element chosen as P_3'. Let $P=(x_1:y_1:1)$ and $Q=(x_2:y_2:1)$ be points of $\varphi(S)\setminus\{P_3'\}$. We will show that $(x_3:y_3:1):=P\oplus Q\in\varphi(S)$; i.e., that $(y_3-1)^{(q+1)/3}\in\mathbf{F}_q$. To see this we can assume that $x_1\neq x_2$ and we have to consider two cases:

Case $P\neq Q$. By the explicit formulas for $\oplus$ (see e.g. [17, p. 28]), we have

$$x_3=-\lambda^2/4-x_1-x_2 \qquad \text{and} \qquad -y_3=\lambda(x_3-x_1)+y_1\,,$$

where $\lambda:=(y_2-y_1)/(x_2-x_1)$. After some computations we find that

$$4(y_3-1)(x_2-x_1)^3=(y_2-y_1)(y_1+y_2-y_1y_2+3)+12x_1x_2^2(y_1+1)-12x_1^2x_2(y_2+1)\,.$$

Let P or Q be either P_1' or P_2'. Then the right hand side of the above identity is either $4(y_1-1)$ or $4(y_2-1)$ and so $(y_3-1)^{(q+1)/3}\in\mathbf{F}_q$. Now let $P,Q\in T$ and let $u_i,v_i\in\mathbf{F}_{q^2}^*$, $i=1,2$, be such that $x_i=1/u_i$, $y_i-1=2v_ix_i^2$, and hence $u_iv_i+u_i^{-1}v_i^2+1=0$, as follows from $y_i^2 = 1 - 4x_i^3$. Let $a_i := u_i v_i$ and $b_i := u_i^{-1} v_i^2$ so that $a_i b_i = v_i^3$ and $a_i + b_i + 1 = 0$. Then

$$12(y_1+1)x_1x_2^2 - 12(y_2+1)x_1^2x_2 = -24(v_1v_2^2 - v_1^2v_2)/a_1^2a_2^2\,, \qquad \text{and}$$
$$(y_2-y_1)(y_1+y_2-y_1y_2+3) = 8(a_1b_2-a_2b_1)(a_1a_2-b_1b_2)\,,$$

so that

$$4(y_3-1)(x_2-x_1)^3 = -8(v_2-v_1)^3/a_1^2a_2^2\,,$$

which shows that $P \oplus Q \in \varphi(S)$.

Case $P = Q$. Here we have (loc. cit.) $x_3 = -\lambda^2/4 - 2x_1$ and y_3 as above, where $\lambda = -6x_1^2/y_1$ (here we can assume that $y_1 \neq 0$). In this case we find that $4(y_3 - 1) = (y_1+1)(y_1-3)^3$ and hence $P \oplus P \in \varphi(S)$. This finishes with Claim 2.

Now the curve $\mathcal{X}$ is $\mathbf{F}_{q^2}$-maximal (see e.g. [2, Corollary 3.7]) and hence $\#\mathcal{J}(\mathbf{F}_{q^2}) = (q+1)^2$ by Remark 1. It follows that $d_S = 3$ by Claims 1 and 2. This shows that $\mathcal{X} = \mathcal{H}_2$ is a curve such that with the set S chosen, satisfies the hypotheses of the Theorem when $q = 5$ or $q = 11$.

§4. Now we give a remark generalizing the Example of the previous section.

Remark 5. The computations we did to prove Claim 1 for $n = 2$ and $q \in \{5, 11\}$ become much more involved for arbitrary n and q such that $d = n^2 - n + 1$ divides $q + 1$. In fact, the set S in the Example always satisfies the hypotheses in the Theorem. This is a consequence of the following general picture of Hurwitz curves $\mathcal{H}_n$ over finite fields. These curves arise early in the mathematical literature being, perhaps, the so-called Klein quartic $\mathcal{H}_3$ the most famous one, see e.g. [8]. The curve $\mathcal{H}_n$ is $\mathbf{F}_{q^2}$-covered by the Fermat curve of degree d; i.e., by the curve $\mathcal{F}_d : X^d + Y^d + Z^d = 0$, via the morphism [3, p. 210]

$$\psi : (X : Y : Z) \mapsto (U : V : W) := (X^nZ : XY^n : YZ^n)\,.$$

We have that $\psi^{-1}(P_1)$ (resp. $\psi^{-1}(P_2)$) (resp. $\psi^{-1}(P_3)$) is the intersection of $\mathcal{F}_d$ with the line $Y = 0$ (resp. $Z = 0$) (resp. $X = 0$). Therefore $\#\psi^{-1}(P_i) = d$ and $\psi^{-1}(P_i) \subseteq \mathcal{F}_d(\mathbf{F}_{q^2})$ for each $i = 1, 2, 3$. Now let $(u : v : 1) \in \mathcal{H}_n$ with $uv \neq 0$, $\eta \in \mathbf{F}_{q^2}$ a d-th root of unity, and let $A_1, \ldots, A_d \in \bar{\mathbf{F}}_{q^2}$ be the roots of $A^d = u^n/v^{n-1}$. Notice that each A_i belongs to $\mathbf{F}_{q^2}$ if and only if at least one A_i belongs. Now it is easy to see that

$$\psi^{-1}(\eta^n u : \eta v : 1) = L_{i,\eta} := \{(A_i y : y : 1) : y^d = u^{-1}v^n\}$$

for some i, so that the covering degree of ψ is d and moreover ψ is unramified.

Claim. *Via the morphism $\psi : \mathcal{F}_d \to \mathcal{H}_n$, each point of S splits completely in $\mathcal{F}_d$.*

We have to show that $\psi^{-1}(S) \subseteq \mathcal{F}_d(\mathbf{F}_{q^2})$. If $(u : v : 1) \in S$, then u^n/v^{n-1} is a d-th power in $\mathbf{F}_{q^2}$ and so all the roots of $A^d = u^n/v^{n-1}$ belong to $\mathbf{F}_{q^2}$, and the claim follows if we show that the equation $Y^d = u^{-1}v^n$ has (at least one) all its roots in $\mathbf{F}_{q^2}$. This follows from the fact that $u^{-1}v^n$ is also a d-th power in $\mathbf{F}_{q^2}$, by the definition of S.

Claim. *The covering ψ is a cyclic cover.*

Let $\tau : (X : Y : Z) \mapsto (\eta X : \eta^n Y : Z)$ on $\mathcal{F}_d$, where η is a primitive d-th root of unity. Then the morphism τ fixes $u = U/W$ and $v = V/W$, so that $\mathbf{F}_{q^2}(\mathcal{H}_n) \subseteq \mathbf{F}_{q^2}(\mathcal{F}_d)^{\langle\tau\rangle}$ and the claim follows.

On the other hand, $\mathcal{F}_d$ is $\mathbf{F}_{q^2}$-maximal, since d divide $q+1$ by hypothesis (indeed this property characterizes the $\mathbf{F}_{q^2}$-maximality of the curve $\mathbf{F}_d$ as well as of the curve $\mathcal{H}_n$ [2, Sect. 3]. Then arguing as in Remark 3 we have that the maximal unramified abelian extension of $\mathcal{H}_n$ in which every point of S splits completely is the Fermat curve $\mathcal{F}_d$ as above. In particular, $d_S = d$. Finally we show that Claim 1 holds. From the definition of ψ above and the computations after it is clear that $L_{i,\eta} \cap \mathcal{F}_d(\mathbf{F}_{q^2}) = \emptyset$ or $L_{i,\eta}$ has exactly d $\mathbf{F}_{q^2}$-rational points of $\mathcal{F}_d$. Then

$$d \cdot (\#S) = \#\mathcal{F}_d(\mathbf{F}_{q^2}) = (q+1)^2 + q(2g'-2) = (q+1)^2 + qd(d-3)\,,$$

and the cardinality of S is as given in Claim 1.

References

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

[2] A. Aguglia, G. Korchmáros and F. Torres, Plane maximal curves. To appear in Acta Arith,

[3] P. Carbonne and T. Henocq, Décomposition de la Jacobienne sur les corps finis. Bull. Polish Acad. Sci. Math. **42**(3), 207–215 (1994).

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

[5] A. Cossidente, G. Korchmáros and F. Torres, Curves of large genus covered by the Hermitian curve. Comm. Algebra **28**(10), 4707–4728 (2000).

[6] R. Fuhrmann, A. Garcia and F. Torres, On maximal curves. J. Number Theory **67**(1), 29–51 (1997).

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

[8] A. Hurwitz, Über die diophantische Gleichung $x^3y + y^3z + z^3x = 0$. Math. Ann. **65**, 428–430 (1908).

[9] G. Korchmáros and F. Torres, On the genus of a maximal curve. arXiv: math.AG/0008202; available at www.ime.unicamp.br/ ftorres.

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

[11] H. Niederreiter and C. Xing, Towers of global function fields with asymptotically many rational places and an improvement on the Gilbert-Varshamov bound. Math. Nachr. **195**, 171–186 (1998).

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

[13] H.G. Rück and H. Stichtenoth, A characterization of Hermitian function fields over finite fields. J. Reine Angew. Math. **457**, 185–188 (1994).

[14] R. Schoof, Algebraic curves over $\mathbf{F}_2$ with many rational points. J. Number Theory **41**, 6–14 (1992).

[15] J.P. Serre, Algebraic groups and class fields. Grad. Texts in Math. Springer, New York, 1988.

[16] J.P. Serre, Rational points on curves over finite fields. Notes by F. Gouvea of lectures at Harvard University, 1985.

[17] J.H. Silverman and J. Tate, Rational points on elliptic curves. Undergrad. Texts Math. Springer, New York, 1992.

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

IBM, Unternehmensberatung, D-40474, Düsseldorf, Germany

E-mail address: rfuhr@de.ibm.com

IMPA, Est. Dna. Castorina 110, Rio de Janeiro, 22.460-320-RJ, Brazil

E-mail address: garcia@impa.br

IMECC-UNICAMP, Cx. P. 6065, Campinas, 13083-970-SP, Brazil

E-mail address: ftorres@ime.unicamp.br