A note on the Giulietti-Korchmáros maximal curve

Arnaldo Garcia

Abstract. We present a very simple proof of the maximality over $\mathbb{F}_{q^6}$ of the curve introduced by Giulietti and Korchmáros in [GK] .

Math. Subject Classification (2000). 11G20, 11D45, 14H50.

Keywords. Rational points, finite fields, Hasse-Weil upper bound, maximal curves.

Introduction

Let $\mathcal{C}$ be a curve (projective, nonsingular and geometrically irreducible) defined over a finite field k, and let $g(\mathcal{C})$ denote its genus.

We have the following bound on the cardinality of the set $\mathcal{C}(k)$ of k-rational points:

$$\#\,\mathcal{C}(k) \leq 1 + \#\,k + 2\sqrt{\#k} \cdot g(\mathcal{C}). \tag{1}$$

The bound above is the so-called Hasse-Weil upper bound. If the cardinality of the finite field is a square, then we say that the curve $\mathcal{C}$ is *maximal* if equality holds in Eq. (1).

Suppose $k = \mathbb{F}_{q^2}$ and $\mathcal{C}$ is maximal. From [Ih] we know that

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

From [RS] we have that the Hermitian curve is the unique maximal curve over $\mathbb{F}_{q^2}$ with genus $g = q(q-1)/2$. The *Hermitian curve* over $\mathbb{F}_{q^2}$ can be given by:

$$X^q + X = Y^{q+1}. \tag{3}$$

It is well-known that subcovers of maximal curves are also maximal, and we have then a natural question:

Question: *Is any maximal curve over* $\mathbb{F}_{q^2}$ *a subcover of the Hermitian curve ?*

Recently Giulietti and Korchmáros introduced a maximal curve over $\mathbb{F}_{q^6}$ which is not a subcover of the corresponding Hermitian curve for $q \neq 2$ (the Hermitian curve is here given by $X^{q^3} + X = Y^{q^3+1}$). Their curve $\mathcal{C}$ over $\mathbb{F}_{q^6}$ is given by (see [GK] and [GGS]):

$$\begin{cases} X^q + X = Y^{q+1} \\ Y^{q^2} - Y = Z^N \text{ with } N = \dfrac{q^3+1}{q+1} \end{cases} \tag{4}$$

The proof in [GK] that $\mathcal{C}$ given by Eq. (4) is maximal over $\mathbb{F}_{q^6}$ is based on the fact that the curve $\mathcal{C}$ lies on a Hermitian surface. In [GGS] we have proved in an elementary way a generalization of this result of [GK]; i.e., we have proved that for an odd integer $n \geq 3$, the curve $\mathcal{C}$ given by Eq. (4) with $N := (q^n+1)/(q+1)$ is maximal over the field $\mathbb{F}_{q^{2n}}$. The proof in [GGS] is based on the fact that the curve χ over $\mathbb{F}_{q^{2n}}$ given by

$$Y^{q^2} - Y = Z^N \quad \text{with} \quad N = \frac{q^n+1}{q+1} \tag{5}$$

is a maximal curve over $\mathbb{F}_{q^{2n}}$ (see [GS] and [ABQ]).

Here we give an even simpler proof of the maximality of the curve $\mathcal{C}$ given by Eq. (4). This new proof is based on the fact that the Hermitian curve given by Eq. (3) is also maximal over $\mathbb{F}_{q^6}$. Since the curve χ over $\mathbb{F}_{q^6}$ given by Eq. (5) with $n = 3$ is a subcover of the curve $\mathcal{C}$, we get as a corollary a simpler proof for the maximality of χ (see [GS]).

The maximality of the curve

The curve $\mathcal{C}$ over $\mathbb{F}_{q^6}$ given by Eq. (4) can also be described by the plane equation:

$$Z^{q^3+1} = \left(\frac{X^{q^2} - X}{X^q + X}\right)^{q+1} \cdot (X^q + X). \tag{6}$$

It follows easily from Eq. (6) that

$$2\, g(\mathcal{C}) = q^5 - 2q^3 + q^2. \tag{7}$$

To prove the maximality of $\mathcal{C}$ over $\mathbb{F}_{q^6}$ we have to show that the following equality holds:

$$\#\, \mathcal{C}(\mathbb{F}_{q^6}) = q^8 - q^6 + q^5 + 1. \tag{8}$$

There are $q+1$ points on $\mathcal{C}$ with $X=\infty$ or $X^q+X=0$; there are $(q^2-q)(q+1)=q^3-q$ points on $\mathcal{C}$ with $X\in\mathbb{F}_{q^2}$ and $X^q+X\neq 0$; all those $q^3+1=(q+1)+(q^3-q)$ points can be shown to be $\mathbb{F}_{q^6}$-rational points on the curve $\mathcal{C}$. Subtracting them from Eq. (8),we have to prove that there are exactly

$$q^8-q^6+q^5-q^3=(q^3+1)\cdot(q^5-q^3)$$

rational points on $\mathcal{C}$ with $Z\in\mathbb{F}_{q^6}$ and $Z\neq 0$. Hence we have to show that

$$\#\left\{X\in\mathbb{F}_{q^6}\middle|\left(\frac{X^{q^2}-X}{X^q+X}\right)^{q+1}\cdot(X^q+X)\in\mathbb{F}_{q^3}^*\right\}=q^5-q^3. \tag{9}$$

Clearly we have that (with $N:=(q^3+1)/(q+1)$):

$$\left(\frac{X^{q^2}-X}{X^q+X}\right)^{q+1}\cdot(X^q+X)=X^{q^3}+X-(X^q-X)^N. \tag{10}$$

Since $X^{q^3}+X$ is the trace from $\mathbb{F}_{q^6}$ to $\mathbb{F}_{q^3}$, from Eq. (10) we have to show that

$$\#\left\{X\in\mathbb{F}_{q^6}\backslash\mathbb{F}_{q^2}\middle|(X^q+X)^N\in\mathbb{F}_{q^3}\right\}=q^5-q^3. \tag{11}$$

To prove this result in Eq. (11) we use that the Hermitian curve $\mathcal{H}$ given by

$$X^q+X=Y^{q+1}$$

is a maximal curve over $\mathbb{F}_{q^6}$ with genus $g=q(q-1)/2$. Hence we know that

$$\#\,\mathcal{H}(\mathbb{F}_{q^6})=q^6+q^5-q^4+1. \tag{12}$$

As before there are (q^3+1) rational points on $\mathcal{H}$ with $X\in\mathbb{F}_{q^2}$ or $X=\infty$. Subtracting them from Eq. (12) we get that there are exactly

$$q^6+q^5-q^4-q^3=(q+1)\cdot(q^5-q^3)$$

$\mathbb{F}_{q^6}$-rational points on $\mathcal{H}$ with $X\in\mathbb{F}_{q^6}\backslash\mathbb{F}_{q^2}$. We then conclude that it holds:

$$\#\left\{X\in\mathbb{F}_{q^6}\backslash\mathbb{F}_{q^2}\middle|(X^q+X)\text{ is a }(q+1)\text{-power in }\mathbb{F}_{q^6}\right\}=q^5-q^3. \tag{13}$$

The proof is now complete since Eq. (11) follows now easily from Eq. (13). Note that

$$N \cdot (q+1) = q^3 + 1$$

is the norm exponent in the extension $\mathbb{F}_{q^6}/\mathbb{F}_{q^3}$. We have then proved:

Theorem. *The curve $\mathcal{C}$ given by Eq. (4) is a maximal curve over $\mathbb{F}_{q^6}$.*

Since the curve χ given by Eq. (5) with $n = 3$ is a subcover of the curve $\mathcal{C}$ we get also:

Corollary. *The curve χ given by Eq. (5) with $n = 3$ is a maximal curve over $\mathbb{F}_{q^6}$.*

References

[ABQ] M. Abdón, J. Bezerra and L. Quoos, *Further examples of maximal curves*, preprint.

[GS] A. Garcia and H. Stichtenoth, *A maximal curve which is not a Galois subcover of the Hermitian curve*, Bull. Braz. Math. Soc. **37** (2006), 139-152.

[GGS] A. Garcia, C. Güneri and H. Stichtenoth, *A generalization of the Giulietti-Korchmáros maximal curve*, preprint.

[GK] M. Giulietti and G. Korchmáros, *A new family of maximal curves over a finite field*, preprint.

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

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

ARNALDO GARCIA
IMPA- Estrada Dona Castorina 110
22460-320, Rio de Janeiro, Brazil.
e-mail: garcia@impa.br