A NOTE ON A MAXIMAL CURVE

Arnaldo Garcia* and Henning Stichtenoth

Abstract. In this note we give a simple proof for the maximality of a curve over a finite field that was recently introduced by Abdon-Bezerra-Quoos. The main ingredient of our proof is a result of Frey-Rück.

1. Introduction

Let k be a finite field of square cardinality $|k| = \ell^2$, with ℓ being some prime power. By definition, a k-maximal curve $\mathcal{C}$ is an algebraic curve (projective, non-singular and geometrically irreducible) defined over k such that its number $|\mathcal{C}(k)|$ of k-rational points attains the Hasse-Weil upper bound; i.e.,

$$|\mathcal{C}(k)| = |k| + 1 + 2g(\mathcal{C})\sqrt{|k|}, \tag{1.1}$$

where $g(\mathcal{C})$ denotes the genus of the curve $\mathcal{C}$. In this note we will be concerned with the case where $\ell = q^n$ and $n \geq 3$ is an odd integer. We fix the following notations:

- $n \geq 3$ is an odd integer,
- q is a power of a prime number p,
- k is the finite field with q^{2n} elements,
- $N := (q^n + 1)/(q + 1)$.

Observe that N is an integer since n is odd.

It is a result due to Abdon-Bezerra-Quoos [1] that the following affine plane equation defines a k-maximal curve:

$$Y^{q^2} - Y = Z^N. \tag{1.2}$$

We denote by χ the curve given by Eqn.(1.2). In [1], the maximality of χ is proved by an explicit determination of the Z-coordinates of the k-rational points, which is in fact very technical and does not give any insight why the curve is maximal. The maximality of χ was later used in [5] to prove that the two equations

$$Y^{q^2} - Y = Z^N \quad \text{and} \quad X^q + X = Y^{q+1} \tag{1.3}$$

define an affine space curve whose non-singular projective model is k-maximal.

*This paper was written while the first author visited Sabanci University in May 2009. His visit was supported by TÜBITAK, Sabanci University and CNPq (Proc. 307569/2006-3).

The particular case $n = 3$ in Eqn.(1.3) is due to Giulietti-Korchmaros [8]. For $q \neq 2$ these curves are particularly interesting since they provide the only examples of maximal curves for which it is known that they are not covered by the Hermitian curve over k.

Maximal curves have the so-called subcover property; i.e., if we have a surjective covering $\mathcal{C}_1 \to \mathcal{C}_2$ defined over k and $\mathcal{C}_1$ is a k-maximal curve, then $\mathcal{C}_2$ is also k-maximal (see [9]).

The Hermitian curve is the best-known maximal curve over k, see [10, Lemma 6.4.4]; it can be defined by the affine plane equation

$$W^{q^n} - W = \alpha X^{q^n+1} \ \text{ with } \ \alpha^{q^n-1} = -1 \ . \tag{1.4}$$

Setting $Z_1 = X^{q+1}$ in Eqn.(1.4) and noting that the element α is an N-th power in the field k, it follows from the subcover property above that also the following equation gives a k-maximal curve:

$$W^{q^n} - W = Z^N \ . \tag{1.5}$$

The aim of this note is to give a simple proof for the maximality of the curve χ in Eqn.(1.2). This will be done by comparing certain subcovers of the curve χ with some subcover of the curve defined by Eqn.(1.5); the latter one we already know to be maximal over k, again by the subcover property of maximal curves. The new ingredient of this simplification is a theorem due to Frey-Rück [3] (see also the appendix of [2]) about relations between Zeta functions in Galois coverings of curves defined over finite fields. Our proof avoids the explicit determination of the Z-coordinates of the rational points in Eqn.(1.2). It would be nice to have a simplification of the proof of the maximality also for the curve in Eqn.(1.3) for $n \geq 5$ (see [4] for the Giulietti-Korchmaros case $n = 3$).

2. Proof of the Theorem

We start with a remark describing a specific quotient curve of the curve given by Eqn.(1.5).

Remark 2.1. Setting in Eqn.(1.5)

$$w := W^{q^n/p} + W^{q^n/p^2} + \cdots + W^p + W \ ,$$

we get that the following equation

$$w^p - w = Z^N \tag{2.1}$$

defines a k-maximal curve.

Now we present our proof of the theorem of Abdon-Bezerra-Quoos [1].

Theorem 2.2. *The curve χ which is defined by the equation*

$$Y^{q^2} - Y = Z^N, \quad N = (q^n + 1)/(q + 1) \ ,$$

is maximal over the field k of cardinality q^{2n}, with $n \geq 3$ odd.

Proof. Denote by $\mathbb{P}^1$ the projective line corresponding to the Z-coordinate. From the defining equation of the curve χ we see that χ covers $\mathbb{P}^1$ and that this covering is p-elementary abelian of degree q^2. We are going to show that all intermediate covers $\mathcal{C}$:

$$\chi \longrightarrow \mathcal{C} \xrightarrow{\varphi} \mathbb{P}^1 \quad \text{with} \quad \deg\varphi = p \ ,$$

are maximal curves over k. After having proved this assertion, the theorem follows immediately from [2, Cor.6.7].
In Eqn.(1.2) we set, for $\beta \in \mathbb{F}_{q^2}^{\times}$,

$$y := (\beta Y)^{q^2/p} + (\beta Y)^{q^2/p^2} + \cdots + (\beta Y)^p + (\beta Y) \ ,$$

then we get the following equation:

$$y^p - y = \beta(Y^{q^2} - Y) = \beta Z^N \ . \tag{2.2}$$

As the element β varies over $\mathbb{F}_{q^2}^{\times}$, the curves given by Eqn.(2.2) are exactly the intermediate curves $\mathcal{C}$ mentioned above, see [6]. Since

$$(q^2-1) \ \text{ divides } \ (q^n-1)\cdot\frac{q^n+1}{N} = (q^n-1)(q+1) \ ,$$

any $\beta \in \mathbb{F}_{q^2}^{\times}$ is in fact an N-th power in the field k. Thus for each $\beta \in \mathbb{F}_{q^2}^{\times}$, the curve $\mathcal{C}$ defined by Eqn.(2.2) is k-isomorphic to the curve given by Eqn.(2.1). Hence all such curves $\mathcal{C}$ are k-maximal, which finishes the proof of the theorem. $\square$

Remark 2.3. It has been shown that the curve over $\mathbb{F}_{3^6}$ given by $Y^9 - Y = X^7$ (which is the special case $q = n = 3$ of Eqn.(1.2)) is not Galois covered by the Hermitian curve over $\mathbb{F}_{3^6}$, see [7]. It seems plausible that this assertion holds for all curves in Eqn.(1.2) with $q \neq 2$. In the case $q = 2$ it is Galois covered, see [1]. A surprizing fact is that both the Hermitian curves and the curves χ from Eqn.(1.2) are fibre products over $\mathbb{P}_1$ of curves which are isomorphic to the one defined by Eqn.(2.1).

Remark 2.4. Using the curve (1.3), one can construct other curves with many rational points as follows. Denote by $\varphi(X)$ the polynomial

$$\varphi(X) := X^{q^3} + X - (X^q + X)^{(q^3+1)/(q+1)} = (X^q + X)\cdot\Big(\frac{X^{q^2} - X}{X^q + X}\Big)^{q+1}. \tag{2.3}$$

Then the maximal curve over $k = \mathbb{F}_{q^{2n}}$ defined by Eqn.(1.3) can also be given by the equation

$$Z^{q^n+1} = \varphi(X). \tag{2.4}$$

The high inseparability of $\varphi(X)$ in Eqn.(2.3) is the key point in showing that the genus γ of the curve given by Eqn.(2.4) is small; we have that

$$2\gamma = (q-1)\cdot(q^{n+1} + q^n - q^2). \tag{2.5}$$

From the maximality of this curve we get

$$\left|\left\{x \in \mathbb{F}_{q^{2n}} \;\middle|\; \varphi(x) \in \mathbb{F}_{q^n}\right\}\right| = q^{n+2} - q^3 + q^2. \tag{2.6}$$

Now we define another curve $\mathcal{C}$ over k by

$$Z^{q^n} + Z = \varphi(X). \tag{2.7}$$

The genus and number of rational points of $\mathcal{C}$ are given by

$$2g(\mathcal{C}) = (q^n - 1)(q^3 - q^2) \;\text{ and }\; |\mathcal{C}(k)| = (q^{n+2} - q^3 + q^2) \cdot q^n + 1 \;, \tag{2.8}$$

where the last equality above follows from Eqn.(2.6). One should also compare the genera in Eqn.(2.5) and Eqn.(2.8). The curve $\mathcal{C}$ is particularly interesting for $q = 2$; in this case one has

$$2g(\mathcal{C}) = 4 \cdot 2^n - 4 \;\text{ and }\; |\mathcal{C}(k)| = 4 \cdot 2^{2n} - 4 \cdot 2^n + 1 \;. \tag{2.9}$$

Note that a maximal curve over k with the genus as in Eqn.(2.9) (if such a curve exists) would have $5 \cdot 2^{2n} - 4 \cdot 2^n + 1$ k-rational points.

References

[1] M. Abdon, J. Bezerra and L. Quoos, *Further examples of maximal curves*, Journal of Pure and Applied Algebra **213** (2009), 1192 - 1196.

[2] I. Duursma, H. Stichtenoth and C. Voss, *Generalized Hamming weights for duals of* BCH *codes, and maximal algebraic function fields*, in *Arithmetic, Geometry and Coding Theory*, R. Pellikaan, M. Perret and S.G. Vladut (Eds.), de Gruyter Berlin-New York (1996), 53-65.

[3] G. Frey and H.-G. Rück, *The strong Lefschetz principle in algebraic geometry*, Manuscr. Math. **55** (1986), 385-401.

[4] A. Garcia, *A note on the Giulietti-Korchmaros maximal curve*, to appear in Proceedings of AGCT-11 (held at CIRM, Marseille, Nov. 2007).

[5] A. Garcia, C. Güneri and H. Stichtenoth, *A generalization of the Giulietti-Korchmaros maximal curve*, to appear in Adv. Geom.

[6] A. Garcia and H. Stichtenoth, *Elementary abelian p-extensions of algebraic function fields*, Manuscr. Math. **72** (1991), 67-79.

[7] 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.

[8] M. Giulietti and G. Korchmaros, *A new family of maximal curves over a finite field*, Math. Ann. **343** (2009), 229–245.

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

[10] H. Stichtenoth, *Algebraic function fields and codes*, 2nd Edition, Graduate Texts in Mathematics **254**, Springer Verlag, 2009.

Arnaldo Garcia, IMPA, Estrada Dona Castorina 110, Rio de Janeiro, Brazil, garcia@impa.br
Henning Stichtenoth, Sabanci University, 34956 Istanbul, Turkey, henning@sabanciuniv.edu