Finite Fields and Their Applications 41 (2016) 72–88

Contents lists available at ScienceDirect

Finite Fields and Their Applications

www.elsevier.com/locate/ffa

On maximal curves that are not quotients of the Hermitian curve

Massimo Giulietti[a,*], Maria Montanucci[b], Giovanni Zini[c]

[a] Dipartimento di Matematica e Informatica, Università degli Studi di Perugia, Via Vanvitelli, 1, 06123 Perugia, Italy
[b] Dipartimento di Matematica, Informatica ed Economia, Università degli Studi della Basilicata, Viale dell'Ateneo Lucano, 10, 85100 Potenza, Italy
[c] Dipartimento di Matematica e Informatica "Ulisse Dini", Università degli Studi di Firenze, Viale Morgagni, 67/a, 50134 Firenze, Italy

ARTICLE INFO

Article history:
Received 30 November 2015
Received in revised form 22 May 2016
Accepted 23 May 2016
Available online 8 June 2016
Communicated by Anne Canteaut

MSC:
11G20

Keywords:
Hermitian curve
Unitary groups
Maximal curves

ABSTRACT

For each prime power ℓ the plane curve $\mathcal{X}_\ell$ with equation $Y^{\ell^2-\ell+1} = X^{\ell^2} - X$ is maximal over $\mathbb{F}_{\ell^6}$. Garcia and Stichtenoth in 2006 proved that $\mathcal{X}_3$ is not Galois covered by the Hermitian curve and raised the same question for $\mathcal{X}_\ell$ with $\ell > 3$; in this paper we show that $\mathcal{X}_\ell$ is not Galois covered by the Hermitian curve for any $\ell > 3$. Analogously, Duursma and Mak proved that the generalized GK curve $\mathcal{C}_{\ell^n}$ over $\mathbb{F}_{\ell^{2n}}$ is not a quotient of the Hermitian curve for $\ell > 2$ and $n \geq 5$, leaving the case $\ell = 2$ open; here we show that $\mathcal{C}_{2^n}$ is not Galois covered by the Hermitian curve over $\mathbb{F}_{2^{2n}}$ for $n \geq 5$.

* Corresponding author.
E-mail addresses: massimo.giulietti@unipg.it (M. Giulietti), maria.montanucci@unibas.it (M. Montanucci), gzini@math.unifi.it (G. Zini).

http://dx.doi.org/10.1016/j.ffa.2016.05.005
1071-5797/

1. Introduction

Let $\mathbb{F}_{q^2}$ be the finite field with q^2 elements, where q is a power of a prime p, and let $\mathcal{X}$ be an $\mathbb{F}_{q^2}$-rational curve, that is a projective, absolutely irreducible, non-singular algebraic curve defined over $\mathbb{F}_{q^2}$. $\mathcal{X}$ is called $\mathbb{F}_{q^2}$-maximal if the number $\mathcal{X}(\mathbb{F}_{q^2})$ of its $\mathbb{F}_{q^2}$-rational points attains the Hasse–Weil upper bound

$$q^2 + 1 + 2gq,$$

where g is the genus of $\mathcal{X}$. Maximal curves have interesting properties and have also been investigated for their applications in Coding Theory. Surveys on maximal curves are found in [9–11,13,32,33] and [23, Chapt. 10].

The most important example of an $\mathbb{F}_{q^2}$-maximal curve is the Hermitian curve $\mathcal{H}_q$, defined as any $\mathbb{F}_{q^2}$-rational curve projectively equivalent to the plane curve with Fermat equation

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

The norm-trace equation

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

gives another model of $\mathcal{H}_q$, $\mathbb{F}_{q^2}$-equivalent to the Fermat model, see [15, Eq. (2.15)]. For fixed q, $\mathcal{H}_q$ has the largest possible genus $g(\mathcal{H}_q) = q(q-1)/2$ that an $\mathbb{F}_{q^2}$-maximal curve can have. The automorphism group $\mathrm{Aut}(\mathcal{H}_q)$ is isomorphic to $\mathrm{PGU}(3,q)$, the group of projectivities of $\mathrm{PG}(2,q^2)$ commuting with the unitary polarity associated with $\mathcal{H}_q$.

By a result commonly attributed to Serre, see [26, Prop. 6], any $\mathbb{F}_{q^2}$-rational curve which is $\mathbb{F}_{q^2}$-covered by an $\mathbb{F}_{q^2}$-maximal curve is also $\mathbb{F}_{q^2}$-maximal. In particular, $\mathbb{F}_{q^2}$-maximal curves are given by the Galois $\mathbb{F}_{q^2}$-subcovers of an $\mathbb{F}_{q^2}$-maximal curve $\mathcal{X}$, that is by the quotient curves $\mathcal{X}/G$ over a finite $\mathbb{F}_{q^2}$-automorphism group $G \leq \mathrm{Aut}(\mathcal{X})$.

Most of the known maximal curves are Galois subcovers of the Hermitian curve, many of which were studied in [4,5,15]. Garcia and Stichtenoth [14] discovered the first example of maximal curve not Galois covered by the Hermitian curve, namely the curve $Y^7 = X^9 - X$ maximal over $\mathbb{F}_{3^6}$. It is a special case of the curve $\mathcal{X}_\ell$ with equation

$$Y^{\ell^2-\ell+1} = X^{\ell^2} - X, \tag{1}$$

which is $\mathbb{F}_{\ell^6}$-maximal for any $\ell \geq 2$; see [1]. In [17], Giulietti and Korchmáros showed that the Galois covering of $\mathcal{X}_\ell$ given by

$$\begin{cases} Z^{\ell^2-\ell+1} = Y^{\ell^2} - Y \\ Y^{\ell+1} = X^\ell + X \end{cases}$$