On maximal curves related to Chebyshev polynomials

Ahmad Kazemifard, Saeed Tafazolian and Fernando Torres

Abstract

We study maximal curves arising from Chebyshev polynomials, where in particular some results from Garcia-Stichtenoth [4] are revisited and generalized.

Keywords: finite field, maximal curves, genus, Chebyshev polynomials.
2000 Mathematics Subject Classification: 11G20, 11M38, 14G15, 14H25.

1 Introduction

Let $\mathcal{C}$ be a (projective, nonsingular, geometrically irreducible algebraic) curve of genus $g = g(\mathcal{C})$ defined over the finite field $\mathbf{F} := \mathbf{F}_{q^2}$ with q^2 elements. Here we will be interested in $\mathbf{F}$-*maximal curves*; i.e., in those curves $\mathcal{C}$ whose number of $\mathbf{F}$-rational points attains the Hasse-Weil upper bound, namely

$$\#\mathcal{C}(\mathbf{F}) = q^2 + 1 + 2gq\,.$$

Apart from being an interesting mathematical object by its own, a maximal curve is often used as a building block in order to obtain outstanding applications in Coding Theory, Cryptography or Finite Geometry; cf. the books [8], [9]. In particular, looking at for handling plane models for maximal curves is a problem of considerable interest nowadays.

In this paper we continue the study in Garcia-Stichtenoth paper [4], where $\mathbf{F}$-maximal curves of Kummer type

$$v^N = F(u)\,, \tag{1}$$

with $F(u)$ being a certain shifted Chebyshev polynomial, were investigated.

Let $\pi : \mathcal{X} \to \mathcal{Y}$ be a dominant $\mathbf{F}$-covering curves over $\mathbf{F}$; then $\mathcal{Y}$ is $\mathbf{F}$-maximal if $\mathcal{X}$ is so (see Remark 3). Now a very well studied $\mathbf{F}$-maximal curve is the Hermitian curve $\mathcal{H}_{q+1}$ [5]; see Equation (2) and Remark 2.

This paper is organized as follows. In Section 2 we recall some preliminary results on maximal curves and on (classical/reduced) Chebyshev polynomials. In Section 3 and Section 4, with $\mathcal{X} = \mathcal{H}_{q+1}$ and certain morphism π, we obtain $\mathbf{F}$-maximal curves defined by polynomials of type (1). Now if instead of $\mathcal{H}_{q+1}$, we use certain generalization $\mathcal{X} = \mathcal{X}(n, \ell, m)$ introduced in Section 2.1 (cf. [20] and [18]) by looking at at certain double coverings we also find $\mathbf{F}$-maximal curves with such plane models. In any case, the results in [4] are widely generalized. In particular, the separability of (reduced) Chebyshev polynomials φ_m is obtained provided that $\gcd(p, m) = 1$ with $p = \mathrm{char}(\mathbf{F})$; see Theorem 22. Previously it was known that φ_m is separable for $m = (q-1)/2$, q odd [4, Thm. 6.1]

Another interesting feature of our paper is the explicit equations that we state for $\mathbf{F}$-maximal elliptic with $q = p$, and $p \not\equiv 1 \mod 24$; see Example 25. For the case $p \equiv 1 \pmod{24}$ see Remark 26.

Notation. Throughout this paper $\mathbb{N}$ stands for the set of positive integers, integers; if $a, b \in \mathbb{N}$, $a \mid b$ means "a divides b"; $\mathbb{P}^t$ is the projective space of dimension t over the algebraic closure of the base field.

2 Preliminaries

2.1 Maximal curves

Let q be a power of a prime and $\mathbf{F}$ be the finite field with q^2 elements. In Curve Theory a very basic object of study is the set

$$\mathbf{M}(q^2) := \{g \in \mathbb{N} : \text{there is an } \mathbf{F}\text{-maximal curve of genus } g\}\,;$$

so far, it is known that $\mathbf{M}(q^2) \subseteq [0, g_2] \cup \{g_1\} \cup \{g_0\}$, where $g_0 := q(q-1)/2)$ (Ihara [10]), $g_1 := \lfloor (q-1)^2/4 \rfloor$ (Fuhrmann-Torres [3]), and $g_2 := \lfloor (q^2 - q + 4)/6 \rfloor$ (Korchmáros-Torres [12]). Now the following plane curve over $\mathbf{F}$

$$\mathcal{H}_{q+1} : \qquad y^{q+1} + x^q = 1\,, \tag{2}$$

the so-called *Hermitian curve over* $\mathbf{F}$, is $\mathbf{F}$-maximal of genus g_0 (see e.g. [15, Ex. 6.3.6]).

Lemma 1. *Notation as above. Let $\mathcal{C}$ be an $\mathbf{F}$-maximal curve of genus $g(\mathcal{C})$. Then*

(1) $g(\mathcal{C}) = g_0$ *if and only $\mathcal{C}$ is $\mathbf{F}$-isomorphic to $\mathcal{H}_{q+1}$* (Rück-Stichtenoth [14]);

(2) $g(\mathcal{C}) = g_1$ *if and only if $\mathcal{C}$ is $\mathbf{F}$-dominated by $\mathcal{H}_{q+1}$ via any involution* ([2], [1], [8, Thm. 10.48]);

(3) $g(C) = g_2$ *only if $\mathcal{C}$ is $\mathbf{F}$-dominated by $\mathcal{H}_{q+1}$ via certain morphism of degree* 3 ([12]).

Remark 2. The Hermitian curve $\mathcal{H}_{q+1}$ above can also be described by equations of type either $y^{q+1} = x^{q+1} + 1$, or $y^{q+1} = x^q + x$ [15, Ex. 6.4.3].

A way of finding elements of $\mathbf{M}(q^2)$ is via the following remark which is commonly attribute to J.P. Serre (cf. [11]):

Remark 3. Any $\mathbf{F}$-subcover of an $\mathbf{F}$-maximal curve is also $\mathbf{F}$-maximal.

Remark 4. There are $\mathbf{F}$-maximal curves which cannot be dominated by the Hermitian curve $\mathcal{H}_{q+1}$ above as the GK-curve shows (Giulietti-Korchmáros [7]; see also Tafazolian et al. [17])

Now let n, ℓ, m be nonnegative integers such that $\gcd(q, nm) = 1$. As a generalization of the Hermitian curve $\mathcal{H}_{q+1}$, we consider the curve $\mathcal{X} := \mathcal{X}(n, \ell, m)$ defined to be the nonsingular model over $\mathbf{F}$ of the plane curve $y^n = x^\ell(x^m + 1)$. By applying Riemann-Hurwitz formula to the separable morphism $x : \mathcal{X} \to \mathbb{P}^1$, the genus $g = g(\mathcal{X})$ satisfies (see e.g. [18, Lemma 2.1])

$$2g = (n-1)m + 2 - \gcd(n, \ell) - \gcd(n, \ell + m)\,. \tag{3}$$

Remark 5. ([18, Remark 2.2]) To work out with the curve $\mathcal{X}(n,\ell,m)$ we can assume $n>\ell$; otherwise, let $\ell=un+r$, $0\le r<n$. Then $\mathcal{X}(n,\ell,m)$ is $\mathbf{F}$-isomorphic to $\mathcal{X}(n,r,m)$ via $(x,y)\mapsto(x,yx^{-u})$.

To deal with the $\mathbf{F}$-rationality of $\mathcal{X}$ we recall that $\mathcal{X}$ is indeed $\mathbf{F}$-covered by the Fermat curve $y^{nm}=x^{nm}+1$ (see e.g. [18, Lemma 2.4]). Then by using Remark 3 we obtain the following:

Lemma 6. *Notation as above. The curve $\mathcal{X}(n,\ell,m)$ is $\mathbf{F}$-maximal if $nm\mid(q+1)$.*

Remark 7. If $n\mid(m+2)$, there is another sufficient condition to ensure the $\mathbf{F}$-maximality of $\mathcal{X}(n,\ell,m)$ whenever $\ell=1$, namely $q\equiv m+1 \pmod{nm}$ [19, Prop. 4.12]; see Section 5 below.

2.2 Chebyshev polynomials

A standard reference to deal with (classical) Chebyshev polynomials is [13]. Let X be a symbol such that $T=X+X^{-1}$ is transcendental over $\mathbb{Z}$, the set of integers, let $m\in\mathbb{N}$. Then by applying the binomial formula in $(X+X^{-1})^m$ and induction on m, there exists a monic polynomial $\Phi_m(T)\in\mathbb{Z}[T]$ of degree m, so called *the m-th Chebyshev polynomial*, such that

$$X^m+X^{-m}=\Phi_m(X+X^{-1})\,.$$

Clearly $\Phi_1(T)=T$ and $\Phi_2(T)=T^2-2$. Let $\Phi_0(T):=2$. From the identity

$$(X+X^{-1})(X^m+X^{-m})=X^{m+1}+X^{-m-1}+X^{m-1}+X^{-m+1}\,,$$

it follows the following recursive formula among Chebyshev polynomials:

$$\Phi_{m+1}(T)=T\Phi_m(T)-\Phi_{m-1}(T)\,,\qquad m\ge 1\,.$$

This was generalized in [4] as follows: For two given polynomials $P_0(T)$, $P_1(T)\in\mathbb{Z}[T]$ define the following (Chebyshev type) recursive formula:

$$P_{k+1}(T)=TP_k(T)-P_{k-1}(T)\,,\qquad k\ge 1\,.$$

Lemma 8. ([4, Thm. 3.1, Remark 3.2])

(1) *If $m=2k+1$, $P_0(T)=1$, $P_1(T)=T+1$, then $\Phi_m(T)-2=(T-2)P_k^2(T)$;*

(2) *If $m=2k+2$, $P_0(T)=1$, $P_1(T)=T+1$, then $\Phi_m(T)-2=(T^2-4)P_k^2(T)$.*

(3) *If $m=2k+1$, $P_0(T)=1$, $P_1(T)=T-1$, then $\Phi_m(T)+2=(T+2)P_k^2(T)$.*

(4) *If $m=2k+2$, $P_0(T)=T$, $P_1(T)=T^2-2$, then $\Phi_m(T)+2=P_k^2(T)$.*

Throughout, as we are working on curves over $\mathbf{F}=\mathbf{F}_{q^2}$, we consider the reduction module $p=\mathrm{char}(\mathbf{F})$ of Φ_m and P_k; we denote such polynomials by φ_m and p_k respectively.

By induction on $m\ge 1$ we can see that Φ_m is separable, in the sense that it has m (distinct) roots in the complex numbers. It is not clear at all that this property still holds true for φ_m over $\bar{\mathbf{F}}$, the algebraic closure of $\mathbf{F}$. In [4, Thm. 6.1], the authors have shown that the polynomial $\varphi_{(q-1)/2}$ is separable for q odd. Here we generalize this result by showing that in fact φ_m is separable whenever $\gcd(p,m)=1$s (see Theorem 22 below).

3 The curve $v^n = \varphi_m(u)$

Throughout this section, q is a power of a prime $p > 2$, $\mathbf{F}$ the finite field with q^2 elements, and $n, m \geq 1$ are integers such that

$$n \mid (q+1)/2, \qquad \text{and} \qquad m \mid (q \pm 1)/2\,.$$

Set $t := (q+1)/2n$ and $s := (q \pm 1)/2m$, and consider the morphism

$$\pi : \mathcal{H} \to \mathbb{P}^2, \qquad (x,y) \mapsto (u : v : 1) := (x^s + x^{-s} : y^{2t}x^{-t} : 1)\,,$$

where $\mathcal{H}$ is the Hermitian curve over $\mathbf{F}$ defined by $y^{q+1} = x^{q+1} + 1$ if $s = (q+1)/2m$, or by $y^{q+1} = x^q + x$ if $s = (q-1)/2m$ (see Remark 2).

Let $\mathcal{C} := \mathcal{C}(n,m)$ be the nonsingular model of the plane curve $\pi(\mathcal{H})$. Recall the definition of the m-th Chebyshev polynomial φ_m over $\mathbf{F}_p$ in Section 2.2.

Theorem 9. *The curve $\mathcal{C}$ above is $\mathbf{F}$-maximal and admits a plane model of type*

$$v^n = \varphi_m(u)\,.$$

Proof. The curve is $\mathbf{F}$-maximal by Remark 3. From $q+1 = 2nt$ and $q+1 = 2ms$,

$$\begin{aligned} v^n &= y^{2nt}x^{-nt} = y^{q+1}x^{-(q+1)/2} = x^{(q+1)/2} + x^{-(q+1)/2} \\ &= (x^s)^m + (x^{-s})^m = \varphi_m(u)\,. \end{aligned}$$

If $q-1 = 2ms$, the proof is similar by taking into consideration that in this case $\mathcal{H}$ is defined by $y^{q+1} = x^q + x$. □

Remark 10. The numerical conditions in Theorem 9 cannot be relaxed; e.g., the curve $v^2 = \varphi_3(u) = u^3 - 3u$ is not $\mathbf{F}_{169}$-maximal as follows by using MAGMA (computational algebraic system).

Remark 11. The case $n = 2$, $q = p$ and $m \geq 5$ prime in Theorem 9 here, was already considered in [16, Ex. 5.3].

Remark 12. By [4, Thm. 6.1] the polynomial $\varphi_{(q-1)/2}(x)$ is separable over $\mathbf{F}_p$; hence $\varphi_m(T)$ is separable provided m divides $(q-1)/2$ as $\varphi_m \circ \varphi_s = \varphi_{ms}$. In particular, for $n \mid (q+1)/2$ and $m \mid (q-1)/2$, $g(\mathcal{C}(n,m)) = (n-1)(m-1)/2$. See Section 7 for further information.

4 The curves $v^n = \varphi_m(u) \pm 2$

Let q be a power of a prime $p \geq 2$, $\mathbf{F}$ the finite field with q^2 elements and $n, m \geq 1$ integers. In this section we consider one of the following conditions:

(A) Both n and m divide $q+1$;

(B) n divides $q+1$ and m divides $q-1$.

Set $q+1 = nt$, $q \pm 1 = ms$ and define the morphism

$$\pi : \mathcal{H} \to \mathbb{P}^2, \qquad (x,y) \mapsto (u : v : 1) := (x^s + x^{-s} : y^{2t}x^{-t} : 1)\,, \tag{4}$$

where $\mathcal{H}$ is the Hermitian curve over $\mathbf{F}$. Let $\mathcal{C}$ be the nonsingular model of the plane curve $\pi(\mathcal{H})$, and recall the definition of the m-th Chebyshev polynomial φ_m over $\mathbf{F}_p$ in Section 2.2.

Theorem 13. *Notation as above. If (A) or (B) holds true, then the curve $\mathcal{C}$ is $\mathbf{F}$-maximal and it can be defined by the plane model*

$$v^n = \varphi_m(u) + 2\,.$$

Moreover, if (B) holds and provided that m is odd, then:

(a) $g(\mathcal{C}) = (n-2)(m-1)/4$, *whenever n is even;*

(b) $g(\mathcal{C}) = (n-1)(m-1)/4$, *whenever n is odd.*

Proof. The curve $\mathcal{C}$ is $\mathbf{F}$-maximal by Remark 3. To compute the plane model we let $\mathcal{H}$ be defined by $y^{q+1} = x^{q+1} + 1$ (resp. $y^{q+1} = x^q + x$) in case A (resp. case (B)); see Remark 2. Then $v^n = \varphi_m(u) + 2$ follows as in the proof of Theorem 9.

Now assume (B) and let $m = 2k+1$. From Lemma 8(3) we have a relation of type $\varphi_m(u) = (u+2)p_k^2(u) - 2$, where in addition $p_k(u)$ is separable with $p_k(-2) \neq 0$ [4, Thm. 6.1]. Then we apply the Riemann-Hurwitz formula to the morphism $u : \mathcal{C} \to \mathbb{P}^1$ and the proof follows after some computations. □

Theorem 14. *Let q be a power of a prime, $n, m \geq 1$ integers satisfying (A) above. Suppose that $m = nd - 2$ with d odd. In this case $\mathcal{C} = \pi(\mathcal{H})$ also admits the plane model:*

$$v^n = \varphi_m(u) - 2\,.$$

Proof. Similar to the proof of Theorem 13. □

Remark 15. The results in this section generalize those in [4, Sect. 4].

5 Double subcovers of $\mathcal{X}(n, \ell, m)$, I

Notation as in Section 2.1; in particular, q is a power of a prime p, $\mathbf{F}$ is the finite field with q^2 elements, $\mathcal{X} := \mathcal{X}(n, \ell, m)$ is the nonsingular model of the plane curve $y^n = x^\ell(x^m + 1)$, where n, ℓ, m are nonnegative integers such that $\gcd(q, nm) = 1$ and $n > \ell \geq 0$. We restrict our attention to the case:

$$m \geq n, \qquad m = nd - 2\ell\,, \quad d \in \mathbb{N}\,.$$

We notice that this condition is related with Remark 7 above. In particular, $\mathcal{X}$ is equipped with the involution

$$\tau_d : (x, y) \mapsto (x^{-1}, yx^{-d})\,;$$

in this section we deal with the double covering

$$\pi_d : \mathcal{X} \to \mathcal{C} := \mathcal{C}(n, \ell, m) := \mathcal{X}/\langle \tau_d \rangle\,. \tag{5}$$

5.1 Case: d even

Theorem 16. *Notation as above and suppose that d is even. If $nm \mid (q+1)$, the curve $\mathcal{C}$ is $\mathbf{F}$-maximal and it is defined by a plane model of type*

$$v^n = \varphi_{m/2}(u)\,,$$

where $\varphi_{m/2}$ is the $m/2$-th Chebyshev polynomial over $\mathbf{F}_p$ as giving in Section 2.2.

In addition, suppose q is odd, $\gcd(n,\ell)=a$ and $\gcd(n,\ell+m)=b$, then

$$g(\mathcal{C}) = \frac{(n-1)(m-2)+2-a-b}{4}.$$

Proof. The curve $\mathcal{C}$ is $\mathbf{F}$-maximal by Lemma 6 and Remark 3. Let us consider the morphism on $\mathcal{X}$

$$\pi = (u,v) := (x+x^{-1}, yx^{-d/2})\,.$$

Then $\pi \circ \tau_d = \pi$ and hence $\pi_d = \pi$; thus the shape of the plane model of $\mathcal{C}$ follows as in the proof of Theorem 9.

To compute the genus we apply Riemann-Hurwitz formula to (5); by (3), $2g(\mathcal{X}) = (n-1)m-a-b$, and the fixed points of τ_d correspond to those $(x,y)\in\mathcal{C}$ such that $x^2=1$ and $y^n=\pm 2$ as d is even. Hence τ_d has $2n$ fixed points, and the claimed genus follows after some computations. □

5.2 Case: d odd

Here we notice that $m \equiv n \pmod 2$. Recall the definition of the polynomials φ_s and p_k given in Section 2.2.

Theorem 17. *Notation as above and suppose that d is odd. If $nm \mid (q+1)$, the curve $\mathcal{C} = \pi_d(\mathcal{X}(n,\ell,m)$ above is $\mathbf{F}$-maximal and it is defined by a plane model of type*

(1) $v^n = (u+2)^{n/2}\varphi_{m/2}(u)$ *whenever n is even;*

(2) $v^n = (u+2)^{(n+1)/2}p_{(m-1)/2}(u)$ *whenever n is odd.*

In addition, suppose q is odd, $\gcd(n,\ell)=a$ and $\gcd(n,\ell+m)=b$, then

(a) $g(\mathcal{C}) = \frac{(n-1)(m-1)+3-a-b}{4}$ *whenever n is even;*

(b) $g(\mathcal{C}) = \frac{(n-1)(m-1)+2-a-b}{4}$ *whenever n is odd.*

Proof. The curve $\mathcal{C}$ is $\mathbf{F}$-maximal by Lemma 6 and Remark 3. Set $d=2k+1$ and so $\varphi_d(T)+2 = (T+2)p_k^2(T)$ by Lemma 8(3).

(1) Let n be even and consider the morphism on $\mathcal{X}$

$$\pi(x,y) = (u,v) := (x+x^{-1}, (y+yx^{-d})/p_k(x+x^{-1}))\,.$$

Then $\pi\circ\tau_d = \pi$ and so $\pi = \pi_d$. Now we obtain the plane models arguing as in Theorem 9; as a matter of fact, let $w := y+yx^{-d}$, then

$$w^n = y^n x^{-dn/2}(x^d+x^{-d}+2)^{n/2} = x^{\ell-nd/2}(x^m+1)(x^d+x^{-d}+2)^{n/2}\,;\quad \text{i.e.,}$$

$$w^n = \varphi_{m/2}(u)(\varphi_d(u) + 2) = \varphi_{m/2}(u)((u + 2)p_k^2(u))^{n/2} .$$

Finally, as $v = w/p_k(u)$, the result follows.

(2) For n odd the proof is similar.

To compute the genus of $\mathcal{C}$ we proceed as in Theorem 13. Here, as d is odd, the fixed points of τ_d are related to the equations $x = 1$, $y^n = 2$, and the point $(-1, 0)$ if n is odd. Thus τ_d has n (resp. $n + 1$) fixed points if n is even (resp. n is odd) and the proof follows after some computations using Riemann-Hurwitz formula applied to (5). □

6 Double subcovers of $\mathcal{X}(n, \ell, m)$, II

Notation as in Section 5. In particular, q is a power of prime $p \geq 2$, $\mathbf{F}$ is the finite field with q^2 elements, and $\mathcal{X} := \mathcal{X}(n, \ell, m)$ is the nonsingular model of the plane curve $y^n = x^\ell(x^m + 1)$, where n, ℓ, m are nonnegative integers such that $\gcd(q, nm) = 1$, $n > \ell \geq 0$, $m \geq n$ and $m = nd - 2\ell$ for certain $d \in \mathbb{N}$. In the following cases, as in Section 5, the curve $\mathcal{X}$ is also equipped with involutions.

(A) n even, or

(B) both n, ℓ odd and d even.

6.1 Case n even

Here $\mathcal{X}$ is equipped with the involution $\tau_d : (x, y) \mapsto (1/x, -y/x^d)$, and we deal with the double coverings

$$\pi_d : \mathcal{X} \to \mathcal{C} = \mathcal{C}_d(n, \ell, m) := \mathcal{X}/\langle\tau_d\rangle . \tag{6}$$

Theorem 18. *Notation as above and suppose that both n and d are even. If $nm \mid (q + 1)$, the curve $\mathcal{C} = \mathcal{C}_d(n, \ell, m)$ is $\mathbf{F}$-maximal and it is defined by a plane model of type*

(1) $v^n = (u - 2)^{n/2}\varphi_{m/2}(u)$ *whenever d is odd;*

(2) $v^n = (u^2 - 4)^{n/2}\varphi_{m/2}(u)$ *whenever d is even,*

where $\varphi_{m/2}$ is the $m/2$-th Chebyshev polynomial over $\mathbf{F}_p$.

Proof. The curve $\mathcal{C}$ is $\mathbf{F}$-maximal by Lemma 6 and Remark 3. Set $d = 2k + 2$ and let $\varphi_d(T) - 2 = (T^2 - 4)p_k^2(T)$ (cf. Lemma 8(2)). Then the morphism (6) above is defined by

$$\pi = (u, v) = (x + x^{-1}, (y - yx^{-d})/p_k(x + x^{-1})) ,$$

as $\pi \circ \tau_d = \pi$; therefore we obtain the claimed plane model as in the proof of Theorem 17. □

Remark 19. In the above theorem, if d is odd, then one can show that the curve $\mathcal{C}$ is also defined by $v^n = (u + 2)^{n/2}\varphi_{m/2}(u)$; cf. Theorem 17(1).

6.2 Case: Both n, ℓ odd and d even

Here m is even and so the curve $\mathcal{X}$ is equipped with the involution $\tau_d : (x,y) \mapsto (-1/x, -y/x^d)$; we deal with the double covering

$$\pi_d : \mathcal{X} \to \mathcal{C} = \mathcal{C}_d(n,\ell,m) := \mathcal{X}/\langle \tau_d \rangle \,. \tag{7}$$

Theorem 20. *Notation as above and suppose that d is even and both n and ℓ are odd. If $nm \mid (q+1)$, the curve $\mathcal{C} = \mathcal{C}_d(n,\ell,m)$ is $\mathbf{F}$-maximal and it is defined by a plane model of type*

$$v^{2n} = (u^2-4)^n \varphi^2_{(m-1)/2}(u)\,,$$

where $\varphi_{(m-1)/2}$ is the $(m-1)/2$-th Chebyshev polynomial over $\mathbf{F}_p$.

Proof. The curve $\mathcal{C}$ is $\mathbf{F}$-maximal by Lemma 6 and Remark 3. To see the claimed plane model, set $d = 2k+2$ and let $\varphi_d(T) = (T^2-4)p_k^2(T) + 2$ (cf. Lemma 8(2)). Then (7) is given by

$$\pi = (u,v) = (x + x^{-1}, (y - yx^{-d})/p_k(x + x^{-1}))\,,$$

as $\pi \circ \tau_d = \pi$; the proof now follows as in Theorem 17. □

7 Further results

Throughout this section, q is a power of a prime $p \geq 2$, $\mathbf{F}$ the finite field with q^2, and n, m nonnegative integers.

Let $\gcd(q, nm) = 1$ and let $\mathcal{X} = \mathcal{X}(n,\ell,m)$ be the curve in Section 2.2 with $\ell = 1$; i.e., the nonsingular model of $y^n = x(x^m+1)$ which was very much studied in [19]. Let us assume the hypotheses in Remark 7:

$$m = dn - 2 \in \mathbb{N}, \qquad q \equiv m+1 \pmod{nm}\,,$$

so that $\mathcal{X}$ is $\mathbf{F}$-maximal. Therefore from the proof of Theorems 16, 17, 18, 20 above, we obtain the following result.

Theorem 21. Let $\gcd(q, nm) = 1$ such that n divides $m+2$. If $q \equiv m+1 \pmod{nm}$, then each of the following equation define a $\mathbf{F}-$maximal curve:

(1) $v^n = \varphi_{m/2}(u)$ if d is even;

(2) $v^n = (u+2)^{n/2}\varphi_{m/2}(u)$ if d is odd and n is even;

(3) $v^n = (u+2)^{(n+1)/2}p_{(m-1)/2}(u)$ if d is odd and n is odd;

(4) $v^n = (u^2-4)^{n/2}\varphi_{m/2}(u)$ if both d and n are even;

(5) $v^{2n} = (u^2-4)^n\varphi^2_{m/2}(u)$ if d is even and n is odd.

In addition, the genus of the nonsingular model $\mathcal{C}$ of each curve above satisfies:

(a) In case (1), $g(\mathcal{C}) = \frac{(n-1)(m-2)}{4}$;

(b) In case (2), $g(\mathcal{C}) = \frac{(n-1)(m-1)+1}{4}$;

(c) In case (3), $g(\mathcal{C}) = \frac{(n-1)(m-1)}{4}$;

(d) In case (4), $g(\mathcal{C}) = \frac{(n-1)m-2}{4}$;

(e) In case (5), $g(\mathcal{C}) = \frac{(n-1)m}{2}$.

Next we will use Theorem 21 to deduce separability properties of the associated (reduced) Chebyshev polynomials φ_t over $\bar{\mathbf{F}}_p$. The following theorem generalizes the results of [4, Thm. 6.1]

Theorem 22. *Let m be an integer such that $gcd(p, m) = 1$. Then*

(a) The m-th Chebyshev polynomial $\varphi_m(T)$ is separable over $\mathbf{F}_p$;

(b) If m divides $(q \pm 1)/2$, then the polynomial $\varphi_m(T)$ having all roots in $\mathbf{F}$;

(c) If m is an odd divisor of $q + 1$, then

$$\varphi_m(T) = (T + 2)p^2(T) - 2\,,$$

where $p(T) \in \mathbf{F}_p[T]$ is a separable polynomial of degree $(m-1)/2$.

Proof. (a) Consider the curve $\mathcal{C}$ given by the equation $v^{m+1} = \varphi_m(u)$. From Theorem 21(a) we get that the genus of $\mathcal{C}$ is $m(m-1)/2$ since we have $2m = 2(m+1) - 2$. On the other hand, we know that the curve $\mathcal{C}$ is a Kummer curve and so by computing also the genus of $\mathcal{C}$ using [15, Prop. 3.7.3], we conclude that $\varphi_m(u)$ is a separable polynomial.

(b) If m divides $(q \pm 1)/2$, then Theorem 9 implies that the curve $v^{(q+1)/2} = \varphi_m(u)$ is $\mathbf{F}$-maximal. By the first part we know that the polynomial $\varphi_m(u)$ is separable and so the desired result follows from [19, Thm. 3.2].

(c) The proof is similar to the part (a) using Theorem 17(b). □

Corollary 23. *Let m be an odd integer or a divisor of $(q \pm 1)/2$. If the curve $v^n = \varphi_m(u)$ is $\mathbf{F}$-maximal, then n divides $q + 1$.*

Proof. If m is odd, then one can show that $\varphi_m(0) = 0$; and if m divides $(q \pm 1)/2$, then by the above theorem we get that φ_m has all roots in $\mathbf{F}$. Hence we conclude that n is a divisor of $q + 1$ from [19, Thm. 3.2] because from Theorem 22 we know that φ_m is a separable polynomial. □

Example 24. Let q be even. As we mention in Lemma 1(2), there is a unique $\mathbf{F}$-maximal curve $\mathcal{C}$ (up to isomorphism) of genus $g(\mathcal{C}) = g_1 = q(q-2)/4$ which in fact can be defined by the Artin-Schreier model $y^{q+1} = x^{q/2} + \ldots + x^2 + x$ (see e.g. [1]). Let $n = q + 1$ and $m = q - 1$. Then according to Theorem 13(b) above the plane equation $v^{q+1} = \varphi_{q-1}(u) + 2$ is also another plane model over $\mathbf{F}$ for $\mathcal{C}$.

Example 25. Here we give explicit examples of maximal elliptic curves over $\mathbf{F}_{p^2}$ for any prime $p \not\equiv 1 \equiv \pmod{24}$.

- $v^2 = \varphi_3(u)$, if $p \equiv 7, 11, 19, 23 \pmod{24}$.
- $v^2 = (u + 2)\varphi_2(u)$, if $p \equiv 5, 13 \pmod{24}$.

- $v^3 = \varphi_2(u)$, if $p \equiv 17 \pmod{24}$.

Remark 26. Let p be a prime with $p \equiv 1 \pmod{73}$. The first value is $p = 73$; for such value, from MAGMA (computational algebraic system), it turns out that the elliptic curve

$$v^2 = u^3 - 3u^2 - 3u + 3 = \varphi_3(u) - 3\varphi_2(u) - 3$$

is $\mathbf{F}_{73^2}$-maximal. This is the only explicit $\mathbf{F}_{p^2}$-maximal elliptic curve we know so far for $p \equiv 1 \pmod{24}$.

Acknowledgments. The second and third author were partially supported respectively by FAPESP/SP-Brazil (Grant 2017/19190-5) and by CNPq-Brazil (Grant 308326/2014-8). The authors heartily thank Daniel Panario for useful conversations on classical Chebyshev polynomials which led to generalize the results in [4].

References

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

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

[3] R. Fuhrmann and F. Torres, *On the genus of curves over finite fields with many rational points*, Manuscripta Math. **89** (1996), 103–106.

[4] A. Garcia and H. Stichtenoth, *On Chebyshev polynomials and maximal curves*, Acta Arith. **90** (1999), 301–311.

[5] A. Garcia, H. Stichtenoth and C. P. Xing, *On subfields of Hermitian function fields*, Composito Math. **120** (2000), 137–170.

[6] A. Garcia and S. Tafazolian, *Certain maximal curves and Cartier operators*, Acta Arith. **135** (2008), 199–218.

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

[8] J.W.P. Hirschfeld, G. Korchmáros and F. Torres, "Algebraic Curves over a Finite Field, Princeton Univ. Press 2008.

[9] N.E. Hurt, "Many Rational Points", Volumen 564 of Mathematics and its Applications, Kluwer 2003.

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

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

[12] G. Korchmáros and F. Torres, *On the genus of maximal curves*, Math. Ann. **323** (2002), 589–608.

[13] T.J. Rivlin, “Chebyshev Polynomials”, Wiley Interscience, New York, Toronto 1990.

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

[15] H. Stichtenoth, “Algebraic function fields and codes”, 2nd edition, Springer 2009.

[16] k. Sugiyama, *On a generalization of Deuring's results*, Finite Fields Appl. **26** (2014), 69–85.

[17] S. Tafazolian, A. Teherán-Herrera and F. Torres, *Further examples of maximal curves which cannot be covered by the Hermitian curve*, J. Pure Appl. Algebra **220** (2016), 1122–1132.

[18] S. Tafazolian and F. Torres, *On the curve* $y^n = x^\ell(x^m+1)$ *over finite fields*, Adv. Geom., to appear.

[19] S. Tafazolian and F. Torres, *On the curve* $y^n = x^m + x$ *over finite fields*, J. Number Theory **145** (2014), 51–66.

[20] B. van Geemen, K. Koike and A. Weng, *Quotients of Fermat curves and a Hecke character*, Finite Fields Appl. **11** (2005), 6–29.

Ahmad Kazemifard
Department of Mathematics,
Faculty of Mathematics and Computer Science,
Shahid Chamran University of Ahvaz, Ahvaz, Iran.
Email: a.kazemifard@scu.ac.ir

Saeed Tafazolian and Fernando Torres
University of Campinas (UNICAMP),
Institute of Mathematics, Statistics and Computer Science (IMECC),
Rua Sérgio Buarque de Holanda, 651, Cidade Universitária,
13083-859, Campinas, SP, Brazil
E-mail: tafazolian@ime.unicamp.br
E-mail: ftorres@ime.unicamp.br