Maximal curves and Tate-Shafarevich results for quartic and sextic twists

Bootsma, Sven; Tafazolian, Saeed; Top, Jaap

Published in:
Finite fields and their applications

DOI:
10.1016/j.ffa.2023.102256

Finite Fields and Their Applications 91 (2023) 102256

Contents lists available at ScienceDirect

Finite Fields and Their Applications

journal homepage: www.elsevier.com/locate/ffa

Maximal curves and Tate-Shafarevich results for quartic and sextic twists

Sven Bootsma [a], Saeed Tafazolian [b,1], Jaap Top [a,*]

[a] *Bernoulli Institute for Mathematics, Computer Science, and Artificial Intelligence, Nijenborgh 9, 9747 AG Groningen, the Netherlands*
[b] *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*

ARTICLE INFO

Article history:
Received 21 December 2022
Received in revised form 14 June 2023
Accepted 15 June 2023
Available online xxxx
Communicated by Gary L. Mullen

MSC:
11G20
11M38
14G15
14H25

Keywords:
Finite field
Maximal curve
Function field
Elliptic curve
Elliptic surface
Mordell-Weil rank

ABSTRACT

We study elliptic surfaces corresponding to an equation of the specific type $y^2 = x^3 + f(t)x$, defined over the finite field $\mathbb{F}_q$ for a prime power $q \equiv 3 \bmod 4$. It is shown that if $s^4 = f(t)$ defines a curve that is maximal over $\mathbb{F}_{q^2}$ then the rank of the group of sections defined over $\mathbb{F}_q$ on the elliptic surface is determined in terms of elementary properties of the rational function $f(t)$. Similar results are shown for elliptic surfaces given by $y^2 = x^3 + g(t)$ using prime powers $q \equiv 5 \bmod 6$ and curves $s^6 = g(t)$. Finally, for each of the forms used here, existence of curves with the property that they are maximal over $\mathbb{F}_{q^2}$ is discussed, as well as various examples.

* Corresponding author.
E-mail addresses: s.bootsma99@gmail.com (S. Bootsma), tafazolian@ime.unicamp.br (S. Tafazolian), j.top@rug.nl (J. Top).

[1] The second author was partially supported by FAPESP grant No. 2022/06589-5 and by CNPq grant No. 310194/2019-9.

https://doi.org/10.1016/j.ffa.2023.102256

1. Introduction and results

Let p be a prime number, let q be a power of p, and denote by $\mathbb{F}_q$ the finite field with q elements and by $\mathbb{F}_{q^2}$ its quadratic field extension. Let $\mathcal{C}$ be a curve (complete, smooth, and geometrically irreducible) of genus $g \geq 0$ defined over $\mathbb{F}_q$. One calls the curve $\mathcal{C}$ maximal over $\mathbb{F}_{q^2}$ if the number of rational points of $\mathcal{C}$ over $\mathbb{F}_{q^2}$ attains the Hasse-Weil upper bound, i.e.,

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

Maximality of $\mathcal{C}$ over $\mathbb{F}_{q^2}$ is equivalent to a property of the Jacobian $\mathcal{J} = \mathcal{J}(\mathcal{C})$ of the curve $\mathcal{C}$: namely, the Frobenius endomorphism $F\colon \mathcal{J} \to \mathcal{J}$ that raises coordinates of points to the power q^2, equals the multiplication by $-q$. This, in turn, is equivalent to the zeta function $Z(\mathcal{C}/\mathbb{F}_{q^2}, T)$ being given as $(1-qT)^{2g}/((1-T)(1-q^2T))$. A consequence of these equivalent characterizations of maximality over $\mathbb{F}_{q^2}$ is that if $\mathcal{C}/\mathbb{F}_{q^2}$ is maximal and $\mathcal{C} \to \mathcal{D}$ is a nonconstant morphism of curves defined over $\mathbb{F}_{q^2}$, then $\mathcal{D}/\mathbb{F}_{q^2}$ is maximal as well. Constructing maximal curves in this way by starting from well-known ones (such as the Hermitian curves over $\mathbb{F}_{q^2}$ given in $\mathbb{P}^2$ by $x^{q+1} + y^{q+1} + z^{q+1} = 0$) remains a popular subject in various papers, see for example [13], [9], [1], [19], [18], [3], [14].

In this note two specific types of curves over $\mathbb{F}_q$ that are maximal over $\mathbb{F}_{q^2}$ are discussed. For the first one, we assume $q \equiv 3 \bmod 4$ which in particular implies that the elliptic curve $E\colon y^2 = x^3 + x$ is maximal over $\mathbb{F}_{q^2}$. In this situation any curve $\mathcal{C}$ over $\mathbb{F}_q$ corresponding to an equation

$$\mathcal{C}\colon s^4 = f(t)$$

such that $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$ is considered. Fix a primitive 4-th root of unity $i \in \mathbb{F}_{q^2}$ and define $\iota \in \mathrm{Aut}(E)$ by $\iota(x, y) = (-x, iy)$. Similarly, $\mu \in \mathrm{Aut}(\mathcal{C})$ denotes the automorphism $\mu(t, s) = (t, is)$. The (minimal resolution of the) quotient $(E \times \mathcal{C})/\langle \iota \times \mu \rangle$ is a surface $\mathcal{E}_f$; its function field is the subfield of $\mathbb{F}_q(x, y, t, s)$ (with $y^2 = x^3 + x$ and $s^4 = f(t)$) consisting of the invariants under $(x, y, t, s) \mapsto (-x, iy, t, is)$. A straightforward verification shows that this field equals $\mathbb{F}_q(\xi, \eta, t)$ where $\xi = s^2x$ and $\eta = s^3y$. The generators satisfy $\eta^2 = \xi^3 + f(t)\xi$. In fact this calculation reflects the observation that the projection $(E \times \mathcal{C})/\langle \iota \times \mu \rangle \to \mathcal{C}/\langle \mu \rangle \cong \mathbb{P}^1$ gives $\mathcal{E}_f$ the structure of an elliptic surface over $\mathbb{P}^1$; it is a quartic twist of the trivial elliptic surface $E \times \mathbb{P}^1 \to \mathbb{P}^1$. The generic fiber of $\mathcal{E}_f \to \mathbb{P}^1$ is the elliptic curve $E_f/\mathbb{F}_q(t)$ with equation $\eta^2 = \xi^3 + f(t)\xi$. In Section 2 we will show the following.

Theorem 1.1. *Suppose $q \equiv 3 \bmod 4$. Take $f(t) \in \mathbb{F}_q(t)$ such that $s^4 = f(t)$ defines a geometrically irreducible curve $\mathcal{C}$ of genus g that is maximal over $\mathbb{F}_{q^2}$.*

Then the rank of the elliptic curve $E_f\colon \eta^2 = \xi^3 + f(t)\xi$ over $\mathbb{F}_q(t)$ equals $g - h$, where h denotes the genus of the hyperelliptic curve corresponding to $s^2 = f(t)$.

In more explicit terms, viewing $f(t)$ as a rational function on $\mathbb{P}^1$ write

$$D_f(\text{odd}) := \{P \in \mathbb{P}^1(\overline{\mathbb{F}_q}) \ : \ \text{ord}_P(f) \equiv 1 \bmod 2\}$$

and

$$D_f(\text{two}) := \{P \in \mathbb{P}^1(\overline{\mathbb{F}_q}) \ : \ \text{ord}_P(f) \equiv 2 \bmod 4\}.$$

The assumption that $s^4 = f(t)$ should define a geometrically irreducible curve $\mathcal{C}$ simply means that $D_f(\text{odd}) \neq \emptyset$. The Zeuthen-Hurwitz genus formula applied to $\mathcal{C} \to \mathbb{P}^1$ defined by $(t, s) \mapsto t$ shows that $2g = 3\#D_f(\text{odd}) + 2\#D_f(\text{two}) - 6$. The same formula applied to the hyperelliptic curve yields $2h = \#D_f(\text{odd}) - 2$. Hence Theorem 1.1 states that provided $\mathcal{C}$ is maximal over $\mathbb{F}_{q^2}$, one obtains

$$\text{rank}\, E_f(\mathbb{F}_q(t)) = \#\left\{P \in \mathbb{P}^1(\overline{\mathbb{F}_q}) \ : \ \text{ord}_P(f) \not\equiv 0 \bmod 4\right\} - 2.$$

A similar result involving specific curves over $\mathbb{F}_q$ that are maximal over $\mathbb{F}_{q^2}$ relates to sextic twists of an elliptic curve. One starts with $E\colon y^2 = x^3 + 1$ and $q \equiv 5 \bmod 6$ so that E is maximal over $\mathbb{F}_{q^2}$. Let $\mathcal{C}$ be a (smooth, geometrically irreducible, projective) curve over $\mathbb{F}_q$, corresponding to an equation $s^6 = g(t)$. Fix $\omega \in \mathbb{F}_{q^2}$ a primitive 3-rd root of unity. One has $\rho \in \text{Aut}(E)$ given by $\rho(x, y) = (\omega x, -y)$ and $\nu \in \text{Aut}(\mathcal{C})$ such that $\nu(t, s) = (t, -\omega s)$. A minimal resolution $\mathcal{E}_g$ of $E \times \mathcal{C}/\langle \rho \times \nu \rangle$ is the surface considered in this case. Its function field is $\mathbb{F}_q(t, \xi, \eta)$ where $\xi = s^3 x$ and $\eta = s^2 y$ hence $\eta^2 = \xi^3 + g(t)$. Here, $\mathcal{E}_g \to \mathcal{C}/\langle \nu \rangle \cong \mathbb{P}^1$ is a sextic twist of $E \times \mathbb{P}^1 \to \mathbb{P}^1$.

Theorem 1.2. *Suppose $q \equiv 5 \bmod 6$. Take $g(t) \in \mathbb{F}_q(t)$ such that $s^6 = g(t)$ defines a geometrically irreducible curve $\mathcal{C}$ of genus g that is maximal over $\mathbb{F}_{q^2}$. For $j \in \{2, 3\}$ write g_j for the genus of the curve corresponding to $s^j = g(t)$.*

The rank of the elliptic curve $E_g\colon \eta^2 = \xi^3 + g(t)$ over $\mathbb{F}_q(t)$ is equal to $g - g_2 - g_3$.

As in the quartic twists case, the genera of the curves occurring here can be read off easily from the rational function $g(t)$: write

$$D_g(\text{odd}) := \{P \in \mathbb{P}^1(\overline{\mathbb{F}_q}) \ : \ \text{ord}_P(g) \equiv \pm 1 \bmod 6\}$$

and

$$D_g(\text{even}) := \{P \in \mathbb{P}^1(\overline{\mathbb{F}_q}) \ : \ \text{ord}_P(g) \equiv \pm 2 \bmod 6\}$$

and

$$D_g(\text{three}) := \{P \in \mathbb{P}^1(\overline{\mathbb{F}_q}) \ : \ \text{ord}_P(g) \equiv 3 \bmod 6\}.$$

The equation $s^6 = g(t)$ defines a geometrically irreducible curve precisely when either $D_g(\text{odd}) \neq \emptyset$ or both of $D_g(\text{even})$ and $D_g(\text{three})$ are nonempty. Under these conditions one obtains

$$\begin{aligned} 2g &= 5\#D_g(\text{odd}) + 4\#D_g(\text{even}) + 3\#D_g(\text{three}) - 10, \\ 2g_2 &= \#D_g(\text{odd}) + \#D_g(\text{three}) - 2, \\ 2g_3 &= 2\#D_g(\text{odd}) + 2\#D_g(\text{even}) - 4. \end{aligned}$$

So whenever $\mathcal{C}/\mathbb{F}_q\colon s^6 = g(t)$ corresponds to a geometrically irreducible curve that is maximal over $\mathbb{F}_{q^2}$, Theorem 1.2 yields

$$\operatorname{rank} E_g(\mathbb{F}_q(t)) = \#\left\{P \in \mathbb{P}^1(\overline{\mathbb{F}_q}) \ : \ \operatorname{ord}_P(g) \not\equiv 0 \bmod 6\right\} - 2.$$

Proofs of Theorems 1.1-1.2 are presented in Section 2. These are variations of a classical idea of Tate and Shafarevich [21], who used Tate's proof [20] of the famous "Tate conjecture for abelian varieties over finite fields" to deduce a result similar to Theorems 1.1-1.2 for the case of quadratic twists. See also [15, §13.3] for a review of the idea by Tate and Shafarevich as well as various examples.

Section 3 discusses examples satisfying the conditions of Theorem 1.1 or Theorem 1.2. As a special case, it turns out that in every characteristic $p \equiv 3 \bmod 4$ taking $q = p^m$ for odd $m \geq 1$, the rank of $\mathcal{E}_{1728}\colon y^2 = x^3 + (t^{q+1} + 1)x$ over $\mathbb{F}_q(t)$ equals $p^m - 1$. This clearly exceeds any given bound when considering $m \gg 0$. Similarly for $p \equiv 5 \bmod 6$ and $q = p^m$ with $m \geq 1$ odd, the rank of $\mathcal{E}_0\colon y^2 = x^3 + t^{q+1} + 1$ over $\mathbb{F}_q(t)$ equals $p^m - 1$. We will discuss how this implies a result of Schütt and Shioda presented in [15, Theorem 13.42], where a rather different argument is used to find the rank of $\mathcal{E}_0$ over the quadratic extension $\mathbb{F}_{q^2}(t)$.

Remark 1.3. The arguments used here exploit that the curves $\mathcal{C}$ are maximal and that the elliptic curve E is supersingular. Arbitrarily high ranks using some *ordinary* elliptic curve E and certain *quadratic* twists of $E \times \mathbb{P}^1 \to \mathbb{P}^1$ are found in [5], [4]. We did not investigate whether the ideas used there extend to the case of quartic or sextic twists.

Remark 1.4. As will be evident from the proofs presented in Section 2, the *geometric* rank, i.e., the rank over $\overline{\mathbb{F}_q}(t)$ of the elliptic curves discussed in Theorems 1.1-1.2, equals twice the rank they have over $\mathbb{F}_q(t)$.

2. Proofs

A first and elementary step in proving Theorems 1.1-1.2 is a reduction to statements over $\mathbb{F}_{q^2}$ instead of $\mathbb{F}_q$. An important advantage will turn out to be that all automorphisms of the elliptic curves in question are defined over $\mathbb{F}_{q^2}(t)$, and also that the extensions of function fields that will be considered are Galois.

Lemma 2.1. *Let K be a field such that $K(i)$ is a quadratic extension of K, where $i^2 = -1$. Let $E\colon y^2 = x^3 + ax$ be an elliptic curve over K.*

Then

$$E(K(i)) \otimes \mathbb{Q} \cong (E(K) \times E(K)) \otimes \mathbb{Q}.$$

In particular, if q is a prime power $\equiv 3 \bmod 4$ and $K = \mathbb{F}_q(t)$, then

$$\operatorname{rank} E(\mathbb{F}_{q^2}(t)) = 2 \cdot \operatorname{rank} E(\mathbb{F}_q(t)).$$

Proof. Define $\iota\colon E \to E$ by $\iota(x, y) = (-x, iy)$ and let σ be the K-linear automorphism of $K(i)$ such that $\sigma(i) = -i$. The action of σ on the coordinates of points in $E(K(i))$ is written as $P \mapsto P^\sigma$. Then $(P, Q) \mapsto P + \iota(Q)$ defines a homomorphism $E(K) \times E(K) \to E(K(i))$ and $R \mapsto (R + R^\sigma, \iota(R^\sigma) - \iota(R))$ is a homomorphism $E(K(i)) \to E(K) \times E(K)$. The composition of the two maps yields multiplication by 2 on $E(K) \times E(K)$, implying the lemma. □

As a consequence of Lemma 2.1, with notations from Theorem 1.1, proving this theorem is equivalent to showing that $\operatorname{rank} E_f(\mathbb{F}_{q^2}(t)) = 2g - 2h$. To achieve the latter equality, the extension $\mathbb{F}_{q^2}(t, s) \supset \mathbb{F}_{q^2}(t)$ will be used, where $s^4 = f(t)$ (so $\mathbb{F}_{q^2}(t, s)$ is the function field of the curve $\mathcal{C}$ over $\mathbb{F}_{q^2}$). By assumption this extension has degree 4. Since $\mathbb{F}_{q^2}$ contains a 4-th root of unity i with $i^2 = -1$, the extension is Galois. Its Galois group is generated by the automorphism

$$\tau\colon \mathbb{F}_{q^2}(t, s) \xrightarrow{\sim} \mathbb{F}_{q^2}(t, s) \text{ defined by } \tau(s) = is.$$

Note that over $\mathbb{F}_{q^2}(t, s)$ the elliptic curves $E\colon y^2 = x^3 + x$ and $E_f\colon y^2 = x^3 + f(t)x$ are isomorphic (reflecting that by construction E_f is a quartic twist of E). Indeed, the map

$$E_f \to E \ : \ (x, y) \mapsto (xs^{-2}, ys^{-3})$$

is an explicit isomorphism. As a consequence one obtains

$$E_f(\mathbb{F}_{q^2}(t)) \subset E_f(\mathbb{F}_{q^2}(t, s)) \cong E(\mathbb{F}_{q^2}(t, s)) = \operatorname{Mor}_{\mathbb{F}_{q^2}}(\mathcal{C}, E).$$

The rank of the latter group equals $4g$, as is well known: indeed, for this one uses the exact sequence (see, e.g., [4, p. 488]; this idea was in fact already used in [21])

$$0 \to E(\mathbb{F}_{q^2}) \longrightarrow \operatorname{Mor}_{\mathbb{F}_{q^2}}(\mathcal{C}, E) \longrightarrow \operatorname{Hom}_{\mathbb{F}_{q^2}}(\mathcal{J}, E) \to 0.$$

Here $\mathcal{J}$ denotes the Jacobian of $\mathcal{C}$; a point $P \in E(\mathbb{F}_{q^2})$ is mapped to the constant morphism with image P, and a morphism $\phi \in \operatorname{Mor}_{\mathbb{F}_{q^2}}(\mathcal{C}, E)$ yields a ϕ_* on divisor classes. The assumption that $\mathcal{C}/\mathbb{F}_{q^2}$ is maximal implies that $\mathcal{J}$ is isogenous over $\mathbb{F}_{q^2}$

to E^g; indeed, maximality of $cC/\mathbb{F}_{q^2}$ is equivalent to the characteristic polynomial of Frobenius attached to $\mathcal{J}/\mathbb{F}_{q^2}$ being $(T+q)^{2g}$ as explained, e.g., in [16, §2.1], see also [11, §10.1]. Since $q \equiv 3 \bmod 4$, the characteristic polynomial of Frobenius on $E^g/\mathbb{F}_{q^2}$ is also $(T+q)^{2g}$. Hence Tate's result [20, Thm 1(c)] proves the existence of an isogeny as stated. As a consequence

$$\begin{aligned}\operatorname{rank} E_f(\mathbb{F}_{q^2}(t,s)) &= \operatorname{rank} \operatorname{Hom}_{\mathbb{F}_{q^2}}(\mathcal{J}, E) = \operatorname{rank} \operatorname{Hom}_{\mathbb{F}_{q^2}}(E^g, E)\\ &= g \cdot \operatorname{rank} \operatorname{End}_{\mathbb{F}_{q^2}}(E) = 4g,\end{aligned}$$

where it is used that the q-th power Frobenius and the map $\iota\colon (x,y) \mapsto (-x, iy)$ do not commute in $\operatorname{End}_{\mathbb{F}_{q^2}}(E)$, implying that $\operatorname{rank} \operatorname{End}_{\mathbb{F}_{q^2}}(E) = 4$.

To complete the proof of Theorem 1.1, the action of τ on $E_f(\mathbb{F}_{q^2}(t,s))$ will be studied in more detail. For convenience, write $V := E_f(\mathbb{F}_{q^2}(t,s)) \otimes \mathbb{Q}$. With $\sqrt{-1} \cdot (P \otimes r) := \iota(P) \otimes r$, this V is actually a vector space over $\mathbb{Q}(\sqrt{-1})$. Moreover τ defines a $\mathbb{Q}(\sqrt{-1})$-linear map $V \to V$ and $\tau^4 = id_V$. We now describe the eigenspaces $V_\lambda \subset V$ corresponding to the 4 possible eigenvalues $\lambda \in \{\pm 1, \pm\sqrt{-1}\}$ of τ.

Clearly eigenvalue $+1$ corresponds to (nontrivial) points $v = P \otimes r$ such that $P^\tau - P$ has finite order, hence some multiple of P is in $E_f(\mathbb{F}_{q^2}(t))$. So $V_1 = E_f(\mathbb{F}_{q^2}(t)) \otimes \mathbb{Q}$.

An element $v = P \otimes r \in V$ to be eigenvector with eigenvalue -1 means that $P^\tau + P$ has finite order. In other words, a multiple of P is of the form $(\xi(t), s^2\eta(t))$ for $\xi(t), \eta(t) \in \mathbb{F}_{q^2}(t)$. This is equivalent to $(f(t)\xi(t), f(t)^2\eta(t)) \in E_{f^3}(\mathbb{F}_{q^2}(t))$ where E_{f^3} denotes the quadratic twist of E_f given by

$$E_{f^3}\colon y^2 = x^3 + f^3 x.$$

It follows that $V_{-1} \cong E_{f^3}(\mathbb{F}_{q^2}(t)) \otimes \mathbb{Q}$. Moreover, since $q \equiv 3 \bmod 4$ the q-power Frobenius morphism defines a rational isogeny $E_f \to E_{f^3}$. In particular, this implies that $E_f(\mathbb{F}_{q^2}(t))$ and $E_{f^3}(\mathbb{F}_{q^2}(t))$ have the same rank, so $\dim V_1 = \dim V_{-1}$.

Next, $V_{\sqrt{-1}}$ is considered. It leads to $P^\tau - \iota(P)$ of finite order and analogous to the cases above, to points $(s^2\xi(t), s\eta(t)) \in E_f(\mathbb{F}_{q^2}(t))$. This means $(f(t)\xi(t), f(t)\eta(t)) \in E_{f^2}(\mathbb{F}_{q^2}(t))$, with

$$E_{f^2}\colon y^2 = x^3 + f^2 x.$$

The rank of $E_{f^2}(\mathbb{F}_{q^2}(t))$ is determined as in the paper [21] of Tate and Shafarevich: write $r = s^2$, so that $\mathbb{F}_{q^2}(t,r)$ is the function field $\mathbb{F}_{q^2}(\mathcal{D})$ of the hyperelliptic curve $\mathcal{D}\colon r^2 = f(t)$ of genus h. Over $\mathbb{F}_{q^2}(\mathcal{D})$ one obtains an isomorphism $E_{f^2} \cong E$, hence as above

$$E_{f^2}(\mathbb{F}_{q^2}(t)) \subset E_{f^2}(\mathbb{F}_{q^2}(t,r)) \cong E(\mathbb{F}_{q^2}(t,r)) = \operatorname{Mor}_{\mathbb{F}_{q^2}}(\mathcal{D}, E).$$

Moreover, since E_{f^2} is the quadratic twist of $E/\mathbb{F}_{q^2}(t)$ using the extension $\mathbb{F}_{q^2}(t,r)/\mathbb{F}_{q^2}(t)$, one obtains $\operatorname{rank} E(\mathbb{F}_{q^2}(t,r)) = \operatorname{rank} E(\mathbb{F}_{q^2}(t)) + \operatorname{rank} E_{f^2}(\mathbb{F}_{q^2}(t)) = \operatorname{rank} E_{f^2}(\mathbb{F}_{q^2}(t))$, as

$E(\mathbb{F}_{q^2}(t)) = \mathrm{Mor}_{\mathbb{F}_{q^2}}(\mathbb{P}^1, E) \cong E(\mathbb{F}_{q^2})$. The inclusion $\mathbb{F}_{q^2}(t,r) \subset \mathbb{F}_{q^2}(t,s)$ corresponds to a degree 2 map $\mathcal{C} \to \mathcal{D}$, implying that $\mathcal{D}$ is maximal over $\mathbb{F}_{q^2}$. Using the validity of the Tate conjecture over finite fields, the Jacobian $\mathcal{J}(\mathcal{D})$ is then isogenous over $\mathbb{F}_{q^2}$ to E^h. The exact sequence

$$0 \to E(\mathbb{F}_{q^2}) \longrightarrow \mathrm{Mor}_{\mathbb{F}_{q^2}}(\mathcal{D}, E) \longrightarrow \mathrm{Hom}_{\mathbb{F}_{q^2}}(\mathcal{J}, E) \to 0$$

now shows

$$\operatorname{rank} E_{f^2}(\mathbb{F}_{q^2}(t)) = \operatorname{rank} E(\mathbb{F}_{q^2}(t,r)) = \operatorname{rank} \mathrm{Mor}_{\mathbb{F}_{q^2}}(\mathcal{D}, E) = \operatorname{rank} \mathrm{Hom}(E^h, E) = 4h.$$

Finally, for $V_{-\sqrt{-1}}$ one considers points $(s^2\xi(t), s^3\eta(t)) \in E_f(\mathbb{F}_{q^2}(t))$, meaning that we have $(\xi(t), \eta(t)) \in E(\mathbb{F}_{q^2}(t)) = E(\mathbb{F}_{q^2})$. The latter group is finite, hence $V_{-\sqrt{-1}} = \{0\}$.

Combining these arguments yields

$$4g = \dim_{\mathbb{Q}}(V) = \dim_{\mathbb{Q}}(V_1) + \dim_{\mathbb{Q}}(V_{-1}) + \dim_{\mathbb{Q}}(V_{\sqrt{-1}}) = 2 \cdot \operatorname{rank} E_f(\mathbb{F}_{q^2}(t)) + 4h.$$

This finishes the proof of Theorem 1.1. □

The proof of Theorem 1.2 presented below follows a mostly identical pattern, so a bit less detail is given. Here a lemma reducing the statement to one over $\mathbb{F}_{q^2}(t)$ is as follows.

Lemma 2.2. *Let K be a field such that $K(\omega)$ is a quadratic extension of K, where ω satisfies $\omega^2 + \omega = -1$. Assume $\mathrm{char}(K) \neq 2$ and let $E\colon y^2 = x^3 + a$ be an elliptic curve over K.*

Then

$$(E(K) \times E(K)) \otimes \mathbb{Q} \cong E(K(\omega)) \otimes \mathbb{Q}.$$

In particular, if q is a prime power $\equiv 5 \bmod 6$ and $K = \mathbb{F}_q(t)$, then

$$\operatorname{rank} E(\mathbb{F}_{q^2}(t)) = 2 \cdot \operatorname{rank} E(\mathbb{F}_q(t)).$$

Proof. Let σ be the nontrivial K-linear automorphism of $K(\omega)$. Note $(\omega - \omega^2)^2 = -3$. The linear action of σ on $E(K(\omega)) \otimes \mathbb{Q}$ decomposes it into a $+1$-eigenspace $E(K) \otimes \mathbb{Q}$ and a -1-eigenspace, generated by elements $(P^\sigma - P) \otimes r$ with $P \in E(K(\omega)) \setminus E(K)$. For such a point P one finds $P^\sigma - P = (\xi, \eta\sqrt{-3})$ with $\xi, \eta \in K$ such that $(9\eta)^2 = (-3\xi)^3 - 27a$. Hence the -1-eigenspace may be identified with $E'(K) \otimes \mathbb{Q}$ where $E'\colon y^2 = x^3 - 27a$. The latter elliptic curve is 3-isogenous to E over K, see, e.g. [23, p. 306]. This implies the result. □

For the remainder of the argument we take, using the notations from the statement of Theorem 1.2, the field extension

$$\mathbb{F}_{q^2}(t) \subset \mathbb{F}_{q^2}(\mathcal{C}) = \mathbb{F}_{q^2}(t, s)$$

with $s^6 = g(t)$. This extension is cyclic of degree 6, with Galois group generated by τ such that $\tau(s) = -\omega s$. One writes

$$W := E_g(\mathbb{F}_{q^2}(t, s)) \otimes \mathbb{Q}.$$

This W is a vector space over $\mathbb{Q}(\zeta_6)$, where ζ_6 denotes a primitive 6-th root of unity, by defining $\zeta_6 \cdot P \otimes r := \rho(-P) \otimes r$. Here $\rho \in \mathrm{Aut}(E_g)$ is defined by $\rho(x, y) = (\omega x, y)$. Analogous to the proof of Theorem 1.1 one has $\dim_{\mathbb{Q}} W = 4g$ with $g = \mathrm{genus}(\mathcal{C})$.

The map τ induces a $\mathbb{Q}(\zeta_6)$-linear automorphism of W. Since $\tau^6 = id$, this leads to a decomposition of W into eigenspaces $W_{\zeta_6^j}$ that will be described now; the verification is straightforward and analogous to the case discussed earlier. For $j \in \mathbb{Z}$ write $E_{g^j} : y^2 = x^3 + g(t)^j$. The result is

$$W_{\zeta_6^j} \cong E_{g^{j+1}}(\mathbb{F}_{q^2}(t)) \otimes \mathbb{Q} \quad \text{for} \quad j = 0, 1, 2, 3, 4$$

and $W_{\zeta_6^5} = \{0\}$. The q-power Frobenius map yields q-isogenies $E_g \to E_{g^q} \cong E_{g^5}$ and $E_{g^2} \to E_{g^{2q}} \cong E_{g^4}$, hence $W_1 \cong W_{\zeta_6^4}$ and $W_{\zeta_6} \cong W_{-1}$. Denoting for $j = 2, 3$ by $\mathcal{C}_j$ the curve of genus g_j given by $y^j = g(x)$. The obvious degree $6/j$ map $\mathcal{C} \to \mathcal{C}_j$ makes $\mathcal{C}_j/\mathbb{F}_{q^2}$ a maximal curve. We use these maps to obtain inclusions $\mathbb{F}_{q^2}(t) \subset \mathbb{F}_{q^2}(\mathcal{C}_j) \subset \mathbb{F}_{q^2}(\mathcal{C})$.

Note that $E_{g^3}(\mathbb{F}_{q^2}(t)) \subset E_{g^3}(\mathbb{F}_{q^2}(\mathcal{C}_2)) \cong \mathrm{Mor}_{\mathbb{F}_{q^2}}(\mathcal{C}_2, E_1)$ and as before, one concludes

$$\dim_{\mathbb{Q}} W_{\zeta_6^2} = \mathrm{rank}\, E_{g^3}(\mathbb{F}_{q^2}(t)) = 4g_2.$$

To analyze the remaining space W_{ζ_6}, the method exploited so far will be used one final time. Write $\mathbb{F}_{q^2}(t) \subset \mathbb{F}_{q^2}(\mathcal{C}_3) = \mathbb{F}_{q^2}(t, r)$ with $r^3 = g(t)$. The Galois group of this extension is generated by ν such that $\nu(r) = \omega r$. The space $U := E_{g^2}(\mathbb{F}_{q^2}(t, r) \otimes \mathbb{Q}$ is a vector space over $\mathbb{Q}(\zeta_6)$ with, as earlier, $\zeta_6 \cdot ((a, b) \otimes q) = (\omega a, -b) \otimes q$. Then ν yields a $\mathbb{Q}(\zeta_6)$-linear map on U, resulting in a decomposition of U into eigenspaces $U_{\zeta_6^{2j}}$. Here $U_1 = E_{g^2}(\mathbb{F}_{q^2}(t)) \otimes \mathbb{Q}$ and one verifies $U_{\zeta_6^4} \cong E_{g^4}(\mathbb{F}_{q^2}(t)) \otimes \mathbb{Q}$ which, using the q-Frobenius, is isomorphic to U_1. Finally, $U_{\zeta_6^2} = \{0\}$. Since $\dim_{\mathbb{Q}} U = 4g_3$, the conclusion is that

$$\dim_{\mathbb{Q}} W_{\zeta_6} = \dim_{\mathbb{Q}} U_1 = \frac{1}{2} \dim_{\mathbb{Q}} U = 2g_3.$$

Finally,

$$4g = \dim_{\mathbb{Q}} W = 2 \dim_{\mathbb{Q}} W_1 + 2 \dim_{\mathbb{Q}} W_{\zeta_6} + \dim_{\mathbb{Q}} W_{\zeta_6^2} = 2 \cdot \mathrm{rank}\, E_g(\mathbb{F}_{q^2}(t)) + 4g_3 + 4g_2.$$

This completes the proof of Theorem 1.2. □

3. Examples

Note that if a curve $\mathcal{C}/\mathbb{F}_q$ admits a degree n map $\mathcal{C} \to \mathbb{P}^1$ defined over $\mathbb{F}_q$, then in particular $\#\mathcal{C}(\mathbb{F}_{q^2}) \leq n(q^2+1)$. Hence if such $\mathcal{C}$ is moreover maximal over $\mathbb{F}_{q^2}$, then its genus g satisfies

$$g \leq \frac{(n-1)(q^2+1)}{2q}.$$

For $q \gg 0$ and fixed n this bound is obviously stronger (although of course only applicable to a small class of curves) in comparison with the main result in [7], which states (at least in characteristic > 2) that apart from curves maximal over $\mathbb{F}_{q^2}$ and isomorphic over $\mathbb{F}_{q^2}$ to one corresponding to $y^q + y = x^m$ with $m \in \{q+1, (q+1)/2\}$, one has

$$g < \frac{(q-1)^2}{4}.$$

The bounds on the genus mentioned here apply in particular to maximal curves corresponding to an equation $s^n = f(t)$, or in more geometric terms, curves over $\mathbb{F}_q$ admitting an automorphism of order n coprime to the characteristic (with the property that any Galois conjugate of the automorphism is a power of it, to ensure that the quotient is again defined over $\mathbb{F}_q$) and such that the quotient by this automorphism has genus 0. In light of Theorems 1.1-1.2 we consider this in two situations:

- $n = 4$ and $q \equiv 3 \bmod 4$;
- $n = 6$ and $q \equiv 5 \bmod 6$.

First, for small q and $n \in \{4, 6\}$ such that $q \equiv -1 \bmod n$ we list integers $g \geq 1$ and curves $\mathcal{C}\colon s^n = f(t)$ of genus g defined over $\mathbb{F}_q$ such that $\mathcal{C}/\mathbb{F}_{q^2}$ is maximal. Next, we discuss some 'families' of examples.

3.1. Small finite fields

The smallest nonempty case is $q = 3$, and in this case only $n = 4$ is relevant here. Using the tables in [10], maximal curves over $\mathbb{F}_9$ of positive genus g only exist for $g = 1$ and $g = 3$. In case $g = 1$ an example is provided by the equation $s^2 = t^3 - t$. Here indeed an automorphism of order $n = 4$ exists, namely $(t, s) \mapsto (-t, is)$ with $i \in \mathbb{F}_9$ satisfying $i^2 = -1$. Then $(s, t) \mapsto r := t^2$ is the corresponding quotient map, and it realizes the curve as a cyclic degree 4 cover of $\mathbb{P}^1$, with equation $s^4 = r(r-1)^2$. By Theorem 1.1, $\mathcal{E}\colon y^2 = x^3 - r(r-1)^2 x$ has rank 1 over $\mathbb{F}_3(r)$. The other case is $g = 3$ and here the Hermitian curve defined using $s^4 = t^4 + 1$ is maximal over $\mathbb{F}_9$. Theorem 1.1 then shows that $\mathcal{E}\colon y^2 = x^3 + (t^4+1)x$ has rank 2 over $\mathbb{F}_3(t)$.

Consider $(q = 5, n = 6)$. Maximal curves over $\mathbb{F}_{25}$ of positive genus g only exist for $g \in \{1, 2, 3, 4, 10\}$. For $g = 10$ the (unique up to $\mathbb{F}_{25}$-isomorphisms) example is the

Hermitian curve $s^6 = t^6 + 1$, and Theorem 1.2 implies that $\mathcal{E}\colon y^2 = x^3 + t^6 + 1$ has rank 4 over $\mathbb{F}_5(t)$. For genus $g = 4$ one uses the quotient of the Hermitian curve by an involution as in [7], so $s^6 = t^3 + 1$. As a consequence, $\mathcal{E}\colon y^2 = x^3 + t^3 + 1$ has rank 2 over $\mathbb{F}_5(t)$. A $g = 2$ example is provided by $s^6 = t^2 + 1$. Also $g = 1$ works: the elliptic curve $E\colon y^2 = x^3 + 1$ is maximal over $\mathbb{F}_{25}$. It admits the automorphism $(x, y) \mapsto (\omega x, -y)$ of order 6, with $\omega \in \mathbb{F}_{25}$ such that $\omega^2 + \omega + 1 = 0$. The quotient map corresponds to $(x, y) \mapsto r := y^2$. Note that $s := xy$ generates $\mathbb{F}_5(E)$ over $\mathbb{F}(r)$, with minimal relation $s^6 = r^3(r-1)^2$. So this is in the required form. The remaining possibility is $g = 3$. The "S_4-model" of the Klein curve, i.e., the plane quartic given by

$$x^4 + y^4 + z^4 + \frac{3 \pm 3\sqrt{-7}}{2}(x^2y^2 + y^2z^2 + z^2x^2) = 0,$$

see [16, §4.1.2], [22, p. 43] is maximal over $\mathbb{F}_{25}$ and of genus 3. However, its automorphism group is the simple group $\mathrm{PSL}(2, \mathbb{F}_7)$ of order 168 and this group does not contain an element of order 6. We claim that in fact no curve $\mathcal{C}$ of genus 3 defined over $\mathbb{F}_5$ by an equation $s^6 = g(t)$ and such that moreover $\mathcal{C}/\mathbb{F}_{25}$ is maximal, exists. Indeed, for a curve of this form to be irreducible and of genus 3, the discussion following Theorem 1.2 implies that $\#D_g(\text{odd}) = \#D_g(\text{three}) = 2$ and $D_g(\text{even}) = 0$. Using this, one is reduced to cases $s^6 = tg_2(t)^3$ where $g_2(t)$ is a monic, separable, quadratic polynomial over $\mathbb{F}_5$ such that $g_2(0) \neq 0$. A simple verification reveals that none of the possibilities results in a curve with number of $\mathbb{F}_5$-rational points equal to 6, a necessary condition for a curve over $\mathbb{F}_5$ to be maximal over $\mathbb{F}_{25}$.

($q = 7$, $n = 4$). The bound $g \leq (n-1)(q^2+1)/(2q)$ here implies $g \leq 10$, which rules out the Hermitian curve (for $q = 7$ of genus 21). The tables [10] plus in case $g = 6$ a result from [2, p. 147] yield as remaining positive possibilities $g \in \{1, 2, 3, 5, 7, 9\}$. For several of these, the examples of maximal genus g curves over $\mathbb{F}_{49}$ found on [10] directly or after a small calculation result in equations of the desired form. They are listed here.

g	curve
1	$s^4 = t(t-1)^2$
2	$s^4 = t(t^2-1)^2$
3	$s^4 = t^4 + 1$
5	$s^4 = t(t^2+1)^3$
9	$s^4 = t^7 + t$.

For $g = 2$ we briefly discuss the entry above. An example (in fact, isomorphic to the one presented in [10]) of a maximal genus 2 curve over $\mathbb{F}_{49}$ is given by $y^2 = x^5 - x$. This admits the order 4 automorphism $(x, y) \mapsto (-x, iy)$ where $i^2 = -1$. The quotient map for this automorphism can be given as $(x, y) \mapsto t := x^2$, resulting, for $s = y$, in the given equation $s^4 = t(t^2-1)^2$ for the curve.

Finally, for $g = 7$ the curve corresponding to $y^{16} = x^9(1-x)$ is maximal over $\mathbb{F}_{49}$. From [6, Thm. 5] it is known that this is in fact the unique example of a maximal genus

7 curve over $\mathbb{F}_{49}$. Although the curve admits automorphisms or order 4, the quotient by any one of them does not have genus 0. In particular, no example $s^4 = f(t)$ exists in this case.

3.2. Families depending on q

The examples for small q presented above, already hint at a few more general cases. We describe some of these here.

In case the positive integer n and the prime power q satisfy $q \equiv -1 \bmod n$, the Hermitian curve $\mathcal{H}/\mathbb{F}_q\colon y^{q+1} = x^{q+1} + 1$ evidently covers the curve $\mathcal{C}\colon s^n = t^{q+1} + 1$ via the map $(x, y) \mapsto (t = x, s = y^{(q+1)/n})$. The curves $\mathcal{H}$ and $\mathcal{C}$ are maximal over $\mathbb{F}_{q^2}$, so from Theorems 1.1-1.2 one obtains the following.

Corollary 3.1. *Take $p \equiv 3 \bmod 4$ a prime number and $q = p^m$ with $m \geq 1$ odd. The elliptic curve $E_{1728}/\mathbb{F}_q(t)\colon y^2 = x^3 + (t^{q+1} + 1)x$ satisfies*

$$\operatorname{rank} E_{1728}(\mathbb{F}_q(t)) = p^m - 1.$$

Corollary 3.2. *Take $p \equiv 5 \bmod 6$ a prime number and $q = p^m$ with $m \geq 1$ odd. The elliptic curve $E_0/\mathbb{F}_q(t)\colon y^2 = x^3 + t^{q+1} + 1$ satisfies*

$$\operatorname{rank} E_0(\mathbb{F}_q(t)) = p^m - 1.$$

Note that the special case $m = 1$ in Corollary 3.2 combined with Lemma 2.2 implies that $\operatorname{rank} E_0(\mathbb{F}_{p^2}(t)) = 2p - 2$ whenever p is a prime number congruent to 5 modulo 6. This is part of the assertion in [15, Theorem 13.42] where a different argument is presented. However, as is also observed in the introduction of [15, §13.3.2] there are similarities between the two approaches: our method (as a variation of the classical one by Tate and Shafarevich [21]) uses that the elliptic surface is covered by the product $\mathcal{H} \times E$ where E denotes the elliptic curve $y^2 = x^3 + 1$. The method of [15] (originating in earlier work [17] by Shioda) may be seen as exploiting the fact that the elliptic surface is covered by the product $\mathcal{H} \times \mathcal{H}$ of Hermitian (Fermat) curves.

With n and $\mathcal{C}\colon s^n = t^{q+1}+1$ as above, for any positive $d|(q+1)$ the curve $\mathcal{C}_d\colon s^n = t^d+1$ is covered by $\mathcal{C}$ and this provides several more examples where one (or depending on q both) of Theorems 1.1-1.2 can be applied.

A similar although slightly more elaborate idea originated in [8] and also results in a quotient of the Hermitian curve $\mathcal{H}$, but only for (n, q) satisfying $q \equiv -1 \bmod 2n$. Recall that for $d \geq 1$ the d-th Chebyshev polynomial is the unique $\varphi_d(x) \in \mathbb{Z}[x]$ such that

$$t^d + t^{-d} = \varphi_d(t + t^{-1})$$

in $\mathbb{Z}[t, t^{-1}]$. One verifies that φ_d is monic and of degree d. Moreover $\varphi_1 = 1$ and $\varphi_2 = x^2-2$ and $\varphi_{d+2}(x) = x\varphi_{d+1}(x)-\varphi_d(x)$ for $d \geq 1$. Also, $\varphi_{ab}(X) = \varphi_a(\varphi_b(X))$. Considering

φ_d as a polynomial in characteristic $p > 0$, it is separable if and only if either $p \nmid 2d$ or $d = 1$, see [18, Lemma 4.1]. Starting from the curve $\mathcal{C}\colon y^n = x^{q+1} + 1$ which is maximal over $\mathbb{F}_{q^2}$, write $q + 1 = 2kn$ (with $k \in \mathbb{Z}_{\geq 1}$ since $q \equiv -1 \bmod 2n$). The map $(x, y) \mapsto (t = x + x^{-1}, s = y/x^k)$ defines a nonconstant morphism $\mathcal{C} \to \mathcal{D}$ where

$$\mathcal{D}\colon s^n = \varphi_{nk}(t).$$

By construction the curve $\mathcal{D}$ is maximal over $\mathbb{F}_{q^2}$; its genus is $(3q - 9)/4$ for $n = 4$, respectively $(5q - 15)/4$ for $n = 6$. The property that if $de = nk$ for $d, e \in \mathbb{Z}_{\geq 1}$ then $\varphi_d(\varphi_e(t)) = \varphi_{nk}(t)$, implies that for such d, e the map $(t, s) \mapsto (\varphi_e(t), s)$ yields a nonconstant morphism $\mathcal{D} \to \mathcal{D}'$ with

$$\mathcal{D}'\colon s^n = \varphi_d(t), \quad d \,|\, nk = (q + 1)/2.$$

This produces several more examples. A specific one of this type is obtained by taking $d = n$ and $e = k$. Since $\varphi_4(x) = x^4 - 4x^2 + 2$ and $\varphi_6(x) = x^6 - 6x^4 + 9x^2 - 2$, it shows that $s^4 = t^4 - 4t^2 + 2$ defines a curve of genus 3 that is maximal over $\mathbb{F}_{q^2}$ whenever $q \equiv -1 \bmod 8$, and similarly $s^6 = t^6 - 6t^4 + 9t^2 - 2$ yields a curve of genus 10 that is maximal over $\mathbb{F}_{q^2}$ for any prime power $q \equiv -1 \bmod 12$. The elliptic surfaces defined using $y^2 = x^3 + \varphi_4(t)x$ and $y^2 = x^3 + \varphi_6(t)$ are in fact rational surfaces. There are well known methods for determining the structure of the group of sections in this case, regardless of the characteristic; see for example [15, Chapters 7-8].

Further examples in the same spirit are obtained by starting from a different model of the Hermitian curve, as follows. See also [8, §4], [12, §3]. As before it is assumed that (q, n) satisfy $q \equiv -1 \bmod 2n$. Choose a positive $d|(q - 1)/2$ and write $q + 1 = 2na$, $q - 1 = 2md$ so that $na = md + 1$. The property $n|(q + 1)$ implies that the curve $\mathcal{C}'\colon y^n = x^q + x$ is maximal over $\mathbb{F}_{q^2}$. A straightforward verification shows that the map $(x, y) \mapsto (t = x^m + x^{-m}, s = yx^{-a})$ defines a nonconstant morphism $\mathcal{C}' \to \mathcal{D}''$ with

$$\mathcal{D}''\colon s^n = \varphi_d(t), \quad d \,|\, (q - 1)/2.$$

Taking $n = 4$ (so that $q \equiv -1 \bmod 8$), the choice $d = (q - 1)/2$ results in a curve of genus $(3q - 9)/4$, and to the elliptic curve over $\mathbb{F}_q(t)$ given by $y^2 = x^3 - \varphi_{(q-1)/2}(t)x$ having rank $(q - 3)/2$ over $\mathbb{F}_q(t)$. Similarly, $n = 6$ and $q \equiv -1 \bmod 12$ and $d = (q - 1)/2$ yield genus $(5q - 15)/4$ and $y^2 = x^3 + \varphi_{(q-1)/2}(t)$ of rank $(q - 3)/2$ over $\mathbb{F}_q(t)$ In both examples, the rank over $\mathbb{F}_{q^2}(t)$ and over $\overline{\mathbb{F}_q}(t)$ equals $q - 3$.

In [12] variations of the constructions used here are discussed, and these result in more explicit cases of similar type. We leave it to the reader to fill in the details for those.

Data availability

Data will be made available on request.

References

[1] Nurdagül Anbar, Alp Bassa, Peter Beelen, A complete characterization of Galois subfields of the generalized Giulietti-Korchmáros function field, Finite Fields Appl. 48 (2017) 318–330.

[2] Nazar Arakelian, Saeed Tafazolian, Fernando Torres, On the spectrum for the genera of maximal curves over small fields, Adv. Math. Commun. 12 (2018) 143–149.

[3] Peter Beelen, Leonardo Landi, Maria Montanucci, Classification of all Galois subcovers of the Skabelund maximal curves, J. Number Theory 242 (2023) 46–72.

[4] Irene I. Bouw, Claus Diem, Jasper Scholten, Ordinary elliptic curves of high rank over $\overline{\mathbb{F}_p}(x)$ with constant j-invariant, Manuscr. Math. 114 (2004) 487–501.

[5] Claus Diem, Jasper Scholten, Ordinary elliptic curves of high rank over $\overline{\mathbb{F}_p}(x)$ with constant j-invariant. II, J. Number Theory 124 (2007) 31–41.

[6] Stefania Fanali, Massimo Giulietti, Irene Platoni, On maximal curves over finite fields of small order, Adv. Math. Commun. 6 (2012) 107–120.

[7] Rainer Fuhrmann, Arnaldo Garcia, Fernando Torres, On maximal curves, J. Number Theory 67 (1997) 29–51.

[8] Arnaldo Garcia, Henning Stichtenoth, On Chebyshev polynomials and maximal curves, Acta Arith. 90 (1999) 301–311.

[9] Arnaldo Garcia, Henning Stichtenoth, Chao-Ping Xing, On subfields of the Hermitian function field, Compos. Math. 120 (2000) 137–170.

[10] Gerard van der Geer, Everett W. Howe, Kristin E. Lauter, Christophe Ritzenthaler, Tables of curves with many points, http://www.manypoints.org, 2009. Retrieved November 28th, 2022.

[11] J.W.P. Hirschfeld, G. Korchmáros, F. Torres, Algebraic Curves over a Finite Field, Princeton Series in Applied Mathematics, Princeton University Press, Princeton, NJ, 2008.

[12] Ahmad Kazemifard, Saeed Tafazolian, Fernando Torres, On maximal curves related to Chebyshev polynomials, Finite Fields Appl. 52 (2018) 200–213.

[13] Gilles 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.

[14] Erik A.R. Mendoza, Luciane Quoos, Explicit equations for maximal curves as subcovers of the BM curve, Finite Fields Appl. 77 (2022) 101945.

[15] Matthias Schütt, Tetsuji Shioda, Mordell-Weil Lattices, Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge (A Series of Modern Surveys in Mathematics), vol. 70, Springer, Singapore, 2019.

[16] Jean-Pierre Serre, Rational Points on Curves over Finite Fields, Documents Mathématiques (Paris), vol. 18, Société Mathématique de France, Paris, 2020. With contributions by Everett Howe, Joseph Oesterlé and Christophe Ritzenthaler, Edited by Alp Bassa, Elisa Lorenzo García, Christophe Ritzenthaler and René Schoof.

[17] Tetsuji Shioda, An explicit algorithm for computing the Picard number of certain algebraic surfaces, Am. J. Math. 108 (1986) 415–432.

[18] Saeed Tafazolian, Jaap Top, On certain maximal hyperelliptic curves related to Chebyshev polynomials, J. Number Theory 203 (2019) 276–293.

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

[20] John T. Tate, Endomorphisms of abelian varieties over finite fields, Invent. Math. 2 (1966) 134–144.

[21] John T. Tate, Igor R. Shafarevich, The rank of elliptic curves, Dokl. Akad. Nauk SSSR 175 (1967) 770–773.

[22] Jaap Top, Hecke L-series related with algebraic cycles or with Siegel modular forms, PhD thesis, University of Utrecht, 1989.

[23] Jaap Top, Descent by 3-isogeny and 3-rank of quadratic fields, in: Advances in Number Theory, Kingston, ON, 1991, in: Oxford Sci. Publ., Oxford Univ. Press, New York, 1993, pp. 303–317.