OPEN ACCESS
Journal of Algebra and Its Applications
Vol. 24, Nos. 13 & 14 (2025) 2541025 (18 pages)

DOI: 10.1142/S0219498825410257

Tate–Shafarevich results for quartic twists in characteristic 2

Herivelto Borges[*,‡], João Paulo Guardieiro[*,§],
Cecília Salgado[†,¶] and Jaap Top[†,‖]

[*]*Instituto de Ciências Matemáticas e de Computação*
Universidade de São Paulo, Avenida Trabalhador São-Carlense
400 — Centro, CEP 13566-590, São Carlos, SP, Brazil

[†]*Bernoulli Institute — Computational & Numerical Mathematics*
Faculty of Science and Engineering (FSE)
University of Groningen, Nijenborgh 9
9747 AG Groningen, The Netherlands
[‡]*hborges@icmc.usp.br*
[§]*joao.guardieiro@usp.br*
[¶]*c.salgado@rug.nl*
[‖]*j.top@rug.nl*

Received 15 May 2024
Accepted 5 August 2024
Published 5 April 2025

Communicated by Peter Beelen

Dedicated to Sudhir Ghorpade, to whom the last author owes many pleasant memories, often at CIRM in Luminy and recently in Hyderabad as well.

The aim of this paper is to present families of elliptic surfaces defined over function fields of even characteristic having arbitrarily large Mordell–Weil rank. More precisely, we study the elliptic surface arising from the quartic twist of a supersingular elliptic curve defined over the field with two elements, using the function field of a maximal curve C admitting an order 4 automorphism. For the resulting elliptic surface, we provide a rank formula for its Mordell–Weil group in terms of the genera of C and another curve covered by C.

Keywords: Finite fields; maximal curves; function fields; elliptic curves; elliptic surfaces; Mordell–Weil rank.

Mathematics Subject Classification 2020: 11G20, 14J27, 14D10, 14G15, 14G17, 14H37

[‖]Corresponding author.

1. Introduction

One of the early applications of Tate's famous "proof of the Tate conjecture in the case of abelian varieties over finite fields" [12], was a less than four pages note [14] by Tate and Shafarevich. The note explained that elliptic curves $E/\mathbb{F}_q(t)$ exist with arbitrarily high rank of the group of rational points $E(\mathbb{F}_q(t))$, for any finite field $\mathbb{F}_q$ of characteristic $\neq 2$. The proof used quadratic twists over $\mathbb{F}_q(t)$, hence the function fields of hyperelliptic curves over $\mathbb{F}_q$. The analogous result in characteristic 2 was added by Elkies [5], who used this case to construct (Mordell–Weil) lattices with very good sphere-packing densities. The exposition in [8, Chap. 13] (in particular, §13.3.1) included an overview of these Tate–Shafarevich results.

In [2], a variant of the approach was presented, using quartic and sextic twists instead of the quadratic ones. This means that the hyperelliptic curves in the original results are replaced by cyclic degree 4 or 6 covers of $\mathbb{P}^1$ [and to allow quartic/sextic twists, only elliptic curves E with $\mathrm{Aut}(E) \neq \{\pm 1\}$ are considered]. The assumption used in [2] was that the characteristic p in which the elliptic curves are considered is either $p \equiv 3 \bmod 4$ or $p \equiv 5 \bmod 6$ (to assure that E is supersingular). At least in the specific example of $E : y^2 = x^3 + t^{p+1} + 1$, this offers an alternative proof of results by Shioda in [9].

The aim of this paper is to extend the methods in [2] to the case of quartic twists in characteristic 2. Specifically, we start (characteristic 2) with $E : y^2 + y = x^3 + x$ and its order 4 automorphism $\iota(x, y) = (x + 1, y + x)$. We take a curve C admitting an automorphism σ of order 4. Then, $(E \times C)/\langle \iota \times \sigma \rangle \to C/\langle \sigma \rangle$ defines an elliptic surface. We describe this surface and we present the conditions allowing us to find the Mordell–Weil rank of the given elliptic surface. In particular, this gives rise to (new) examples over $\mathbb{F}_{2^n}(t)$ of arbitrarily high rank.

2. Preliminaries

This section reviews the properties of a specific (supersingular) elliptic curve defined over $\mathbb{F}_2$. Moreover, the special case "characteristic 2" of a result by Artin and Schreier [1] is recalled, describing all field extensions $L \supset K$ of degree p^2 in characteristic $p > 0$ that are Galois with a cyclic Galois group. We also cite a consequence of Tate's result [12] on endomorphisms of abelian varieties over finite fields important in the presented approach. Finally, our rank formula is presented. Its proof and various examples are described in the remaining sections.

The elliptic curve $E/\mathbb{F}_2 : y^2 + y = x^3 + x$ admits the automorphism ι given by $\iota(x, y) = (x + 1, y + x)$. One verifies $\iota^2 = [-1]$, which implies that ι has order 4. It is related to the Frobenius endomorphism F on E given by $F(x, y) = (x^2, y^2)$ via $F = [-1] + \iota$. As a consequence,

$$\#E(\mathbb{F}_{2^{2n}}) = \deg([1] - F^{2n}) = \begin{cases} 2^{2n} + 1 & \text{if } n \equiv 1 \bmod 2, \\ (2^n - 1)^2 & \text{if } n \equiv 0 \bmod 4, \\ (2^n + 1)^2 & \text{if } n \equiv 2 \bmod 4. \end{cases}$$

In particular, this shows that $E/\mathbb{F}_{2^{2n}}$ is maximal precisely when $n \equiv 2 \bmod 4$, respectively minimal if and only if $n \equiv 0 \bmod 4$. Recall that a (smooth, complete, geometrically irreducible) curve $C/\mathbb{F}_{q^2}$ of genus g is maximal iff $\#C(\mathbb{F}_{q^2}) = q^2 + 1 + 2gq$, respectively minimal iff $\#C(\mathbb{F}_{q^2}) = q^2 + 1 - 2gq$ (compare e.g. [11, Definition 5.3.2]).

The results in this paper use non-constant morphisms $C \to X$ defined over $\mathbb{F}_q$, where C, X are curves and q is a power of 2. This is done assuming that the corresponding extension $\mathbb{F}_q(C) \supset \mathbb{F}_q(X)$ is Galois with cyclic Galois group of order 4. In other words, C admits an automorphism σ of order 4 and $X = C/\langle\sigma\rangle$ (and the morphism $C \to X$ is the quotient map). As a special case of [1, Sec. 2], Artin and Schreier described all such extensions: take $A \in \mathbb{F}_q(X)\backslash\wp(\mathbb{F}_q(X))$, where $\wp : f \mapsto f^2 + f$. Take any $B \in \mathbb{F}_q(X)$. Then, $\mathbb{F}_q(C) = \mathbb{F}_q(X)[r, s]$ with $r^2 + r = A$ and $s^2 + s = rA + B$. In this form, the automorphism σ is determined by

$$\sigma(s) = s + r, \quad \sigma(r) = r + 1. \tag{1}$$

One has the "intermediate" curve $H := C/\langle\sigma^2\rangle$ with the function field $\mathbb{F}_q(H) = \mathbb{F}_q(X)[r]$, and the morphisms of degree 2

$$C \to H \to X.$$

Using these notations, our main result states the following.

Theorem 1. *Let $E_{A,B}/\mathbb{F}_{q^2}(X)$ be defined by the Weierstrass equation*

$$y^2 + y = x^3 + Ax^2 + (A + 1)x + A^2 + B.$$

Assume that both $C/\mathbb{F}_{q^2}$ and $E/\mathbb{F}_{q^2}$ are maximal (*or both minimal*). *Then,*

$$\operatorname{rank} E_{A,B}(\mathbb{F}_{q^2}(X)) = 2g(C) - 2g(H),$$

where $g(C)$ and $g(H)$ denote the genera of the curves C and H, respectively.

An ingredient in the proof (and similarly in other instances of the Tate–Shafarevich approach) is the determination of $\operatorname{rank} E(\mathbb{F}_{q^2}(D))$ for a curve $D/\mathbb{F}_{q^2}$, assuming that both D and E are maximal over $\mathbb{F}_{q^2}$ (respectively, both minimal). Identifying $E(\mathbb{F}_{q^2}(D))$ with $\operatorname{Mor}_{\mathbb{F}_{q^2}}(D, E)$, the Albanese property of a Jacobian, yields an exact sequence

$$0 \to E(\mathbb{F}_{q^2}) \to \operatorname{Mor}_{\mathbb{F}_{q^2}}(D, E) \to \operatorname{Hom}_{\mathbb{F}_{q^2}}(\operatorname{Jac}(D), E) \to 0.$$

Hence, $\operatorname{rank} E(\mathbb{F}_{q^2}(D)) = \operatorname{rank} \operatorname{Hom}_{\mathbb{F}_{q^2}}(\operatorname{Jac}(D), E)$. The maximality condition on D and E implies that the characteristic polynomials denoted by f_E and $f_{\operatorname{Jac}(D)}$ in Tate's paper [12] equal $(T + q)^2$ and $(T + q)^{2g(D)}$ (and q replaced by $-q$ in the minimal case). It hence [12, Theorem 1(a)] implies

$$\operatorname{rank} E(\mathbb{F}_{q^2}(D)) = 4 \cdot g(D).$$

3. The Quartic Twist

In this section, we explain the explicit equation for $E_{A,B}$ appearing in Theorem 1. Fix q and curves C, X over $\mathbb{F}_q$ and $\sigma \in \mathrm{Aut}_{\mathbb{F}_q}(C)$ determined by $A, B \in \mathbb{F}_q(X)$ as in Sec. 2. Using moreover the elliptic curve E and its automorphism ι, the projection $E \times C \to C$ induces a morphism

$$(E \times C)/\langle \iota \times \sigma \rangle \to C/\langle \sigma \rangle = X.$$

We will show that this defines an elliptic surface over X, in fact by establishing that its generic fiber is the elliptic curve $E_{A,B}/\mathbb{F}_q(X)$. This is done by determining the subfield $\mathbb{F}$ of $\mathbb{F}_q(X)(x, y, r, s)$ of elements fixed by the action of the automorphism $\iota \times \sigma$. Since

$$\iota \times \sigma : (x, y, r, s) \mapsto (x + 1, y + x, r + 1, s + r),$$

it is easy to see that $x + r$, $x^2 + x$ belong to $\mathbb{F}$. We then have

$$\mathbb{F}_q(X)(x + r, x^2 + x) \subseteq \mathbb{F} \subseteq \mathbb{F}_q(X)(x, y, r, s).$$

As a consequence, $\iota \times \sigma$ yields an $\mathbb{F}_q(X)(x + r, x^2 + x)$-linear map. Consider the chain of field extensions

$$\mathbb{F}_q(X)(x + r, x^2 + x) \subseteq \mathbb{F}_q(X)(x, r) \subseteq \mathbb{F}_q(X)(x, y, r) \subseteq \mathbb{F}_q(X)(x, y, r, s).$$

Each consecutive extension is of degree 2 (because of the equations for E and C). Hence, $\mathbb{F}_q(X)(x, y, r, s)$ has degree 8 and the basis

$$\{1, x, y, xy, s, xs, ys, xys\}$$

over $\mathbb{F}_q(X)(x + r, x^2 + x)$. In terms of this basis, the automorphism $\iota \times \sigma$ is represented by the 8×8 matrix

$$\begin{pmatrix}
1 & 1 & 0 & x^2+x & x+r & x^2+r & x^2+x & (x^2+x)(x+r) \\
0 & 1 & 1 & 0 & 1 & x+r & x+r+1 & x^2+x \\
0 & 0 & 1 & 1 & 0 & 0 & x+r & x^2+r \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & x+r \\
0 & 0 & 0 & 0 & 1 & 1 & 0 & x^2+x \\
0 & 0 & 0 & 0 & 0 & 1 & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 1
\end{pmatrix}.$$

The eigenspace associated to the eigenvalue 1 (i.e. the elements fixed by the automorphism) consists of the vectors

$$(a_1, (x + r)a_s, a_s, 0, a_s, 0, 0, 0).$$

It follows that $[\mathbb{F} : \mathbb{F}_q(X)(x + r, x^2 + x)] = 2$ and a basis for $\mathbb{F}$ over $\mathbb{F}_q(X)(x + r, x^2 + x)$ is given by $\{1, (x + r)x + y + s\}$. Let

$$\eta = (x^2 + r) \cdot 1 + 1 \cdot ((x + r)x + y + s) = y + rx + r + s \quad \text{and} \quad \xi = x + r.$$

Since $\xi^2 + \xi = x^2 + r^2 + x + r = x^2 + x + A$, the elements ξ and η generate the field $\mathbb{F}$ over $\mathbb{F}_q(X)$. One computes

$$\eta^2 = y^2 + r^2(x^2+1) + s^2 = y^2 + (r+A)(x^2+1) + s^2$$

and

$$\eta^2 + \eta = x^3 + (r+A)x^2 + (r+1)x + (r+1)A + B.$$

Since

$$\xi^3 = x^3 + rx^2 + r^2x + r^3 = x^3 + rx^2 + (r+A)x + (r+1)A + r,$$

it follows that

$$\eta^2 + \eta + \xi^3 = Ax^2 + (A+1)x + r = A(x^2+x) + x + r + B.$$

Finally, the relation

$$x^2 + x = \xi^2 + \xi + A$$

results in

$$\eta^2 + \eta = \xi^3 + A\xi^2 + (A+1)\xi + A^2 + B, \tag{2}$$

which is the defining equation of $E_{A,B}$ over $\mathbb{F}_q(X)$. Note that the j-invariant of $E_{A,B}$ is 0 [as is obvious by construction, namely the degree 4 base change $C \to X$ results in the isotrivial elliptic surface $E \times C \to C$ with generic fiber E over $\mathbb{F}_q(C)$]. Explicitly, by construction,

$$\begin{aligned} E &\simeq E_{A,B}, \\ (\xi + r, \eta + r\xi + A + s) &\leftarrow\!\shortmid (\xi, \eta), \\ (x, y) &\mapsto (x + r, y + rx + r + s). \end{aligned} \tag{3}$$

The discriminant of the Weierstrass equation for $E_{A,B}$ equals 1. Hence, only at the pole(s) of the functions A, B the elliptic surface over X may have singular fibers.

4. The Proof of Theorem 1

The automorphism ι on E induces an automorphism on $E_{A,B}$ which we again denote by ι, namely

$$\iota : (\xi, \eta) \mapsto (\xi + 1, \eta + \xi).$$

Note that $\iota^2 = [-1]$. Let C be the curve discussed in Sec. 2 (and in particular, in Theorem 1). Then,

$$V = E_{A,B}(\mathbb{F}_{q^2}(C)) \otimes \mathbb{Q}$$

is in fact a $\mathbb{Q}(i)$-vector space, by setting

$$i \cdot (P \otimes a) = \iota(P) \otimes a.$$

The automorphism σ given in Eq. (1) induces a $\mathbb{Q}(i)$-linear map $\tau : V \to V$ as follows: Write

$$P = (x_0 + x_1r + x_2s + x_3rs, y_0 + y_1r + y_2s + y_3rs),$$

with $x_j, y_j \in \mathbb{F}_q(X)$, then

$$\begin{aligned}\tau(P \otimes a) = (&x_0 + x_1 + x_3 A + (x_1 + x_2)r + (x_2 + x_3)s + x_3 rs,\\ &y_0 + y_1 + y_3 A + (y_1 + y_2)r + (y_2 + y_3)s + y_3 rs) \otimes a.\end{aligned}$$

Note that $\mathbb{Q}(i)$-linearity follows from $\iota \circ \tau = \tau \circ \iota$ on V.

We will use τ to decompose V as the sum of eigenspaces. Since $\tau^4 = id_V$, the eigenvalues of τ are contained in $\{\pm 1, \pm i\}$, hence

$$V = \mathrm{Ker}(\tau - id_V) \oplus \mathrm{Ker}(\tau + id_V) \oplus \mathrm{Ker}(\tau - i \cdot id_V) \oplus \mathrm{Ker}(\tau + i \cdot id_V).$$

We will now study each eigenspace:

- $\mathrm{Ker}(\tau - id_V)$: Comparing the coordinates, one sees that $0 \neq P \otimes a \in \mathrm{Ker}(\tau - id_V)$ if and only if

  $$P \otimes a = (x_0, y_0) \otimes a,$$

  with $(x_0, y_0) \in E_{A,B}(\mathbb{F}_{q^2}(X))$. Therefore, this eigenspace is precisely $E_{A,B}(\mathbb{F}_{q^2}(X)) \otimes \mathbb{Q}$. In particular,

  $$\dim_{\mathbb{Q}} \mathrm{Ker}(\tau - id_V) = \mathrm{rank}\, E_{A,B}(\mathbb{F}_{q^2}(X)).$$

- $\mathrm{Ker}(\tau + id_V)$: Here, $0 \neq P \otimes a \in \mathrm{Ker}(\tau + id_V)$ if and only if

  $$P \otimes a = (x_0, y_0 + r) \otimes a,$$

  with $(x_0, y_0 + r) \in E_{A,B}$ and $x_0, y_0 \in \mathbb{F}_{q^2}(X)$. From the isomorphism between E and $E_{A,B}$ given in Eq. (3), it follows that those points on E correspond to the points of the form

  $$(x_0 + r, y_0 + r + rx_0 + A + s).$$

  From [10, Proposition A.1.2], we know that the automorphism group of E consists of the automorphisms

  $$(x, y) \mapsto (u^2 x + \alpha, y + u^2 \alpha^2 x + \beta),$$

  where

  $$u^3 = 1, \quad \alpha^4 + \alpha = u^2 + 1, \quad \beta^2 + \beta + \alpha^3 + \alpha = 0.$$

  Choose $u = 1$, $\alpha \in \mathbb{F}_4 \backslash \mathbb{F}_2$ and β any root of $\beta^2 + \beta = \alpha^3 + \alpha = 1 + \alpha$ (which is an element of $\mathbb{F}_{16} \backslash \mathbb{F}_4$). The assumption that $E/\mathbb{F}_{q^2}$ is either maximal or minimal, implies that the automorphism given by u, α, β is defined over $\mathbb{F}_{q^2}$. Composing it with the isomorphism given in Eq. (3), one obtains

  $$(x_0 + r, y_0 + r + rx_0 + A + s) \mapsto (x_0 + \alpha, y_0 + (\alpha + 1)x_0 + \beta).$$

  The resulting points are invariant under the action of σ, so $\mathrm{Ker}(\tau + id_V)$ can be identified with a subspace of $\mathrm{Ker}(\tau - id_V)$ and therefore,

  $$\dim_{\mathbb{Q}} \mathrm{Ker}(\tau + id_V) \leq \dim_{\mathbb{Q}} \mathrm{Ker}(\tau - id_V).$$

On the other hand, starting from a point $(x_0, y_0) \otimes a \in \mathrm{Ker}(\tau - id_V)$, the same procedure with the same isomorphisms shows

$$\dim_{\mathbb{Q}} \mathrm{Ker}(\tau - id_V) \leq \dim_{\mathbb{Q}} \mathrm{Ker}(\tau + id_V)$$

and so, one concludes

$$\dim_{\mathbb{Q}} \mathrm{Ker}(\tau + id_V) = \dim_{\mathbb{Q}} \mathrm{Ker}(\tau - id_V) = \mathrm{rank}\, E_{A,B}(\mathbb{F}_{q^2}(X)).$$

- $\mathrm{Ker}(\tau - i \cdot id_V)$: Now, we have $P \otimes a$ in this eigenspace if and only if

$$P \otimes a = (x_0 + r, y_0 + x_0 \cdot r + s) \otimes a,$$

with $(x_0 + r, y_0 + x_0 \cdot r + s) \in E_{A,B}$ and $x_0, y_0 \in \mathbb{F}_{q^2}(X)$. This translates into the condition that (x_0, y_0) is an $\mathbb{F}_{q^2}(X)$-rational point on the elliptic curve

$$E_H : y^2 + y = x^3 + x + A.$$

As in Sec. 2, let $H \to X$ be the curve corresponding to $r^2 + r = A$. Over $\mathbb{F}_q(H)$ we have $E \simeq E_H$, in fact, an isomorphism (and its inverse mapping) is given by $(x, y) \mapsto (x, y + r)$. In other words, E_H is a quadratic twist of $E/\mathbb{F}_q(X)$, see e.g. [5; 3, Sec. 3] for similar examples. The assumption that both C and E are maximal over $\mathbb{F}_{q^2}$ (or both minimal) implies that the same holds for both H and E. Hence, as explained in Sec. 2,

$$\mathrm{rank}\, E_H(\mathbb{F}_{q^2}(H)) = \mathrm{rank}\, E(\mathbb{F}_{q^2}(H)) = 4g(H).$$

The curve E_H being a quadratic twist of $E/\mathbb{F}_{q^2}(X)$ implies in particular that

$$\mathrm{rank}\, E_H(\mathbb{F}_{q^2}(H)) = \mathrm{rank}\, E_H(\mathbb{F}_{q^2}(X)) + \mathrm{rank}\, E(\mathbb{F}_{q^2}(X)),$$

as is shown by decomposing the group up to a finite index into eigenspaces (with eigenvalues $+1$ and -1) for the action of $\mathrm{Gal}(\mathbb{F}_{q^2}(H)/\mathbb{F}_{q^2}(X))$. Reasoning as before yields

$$\mathrm{rank}\, E_H(\mathbb{F}_{q^2}(X)) = 4g(H) - \mathrm{rank}\, E(\mathbb{F}_{q^2}(X)) = 4g(H) - 4g(X),$$

leading to the conclusion

$$\dim_{\mathbb{Q}} \mathrm{Ker}(\tau - i \cdot id_V) = \mathrm{rank}\, E_H(\mathbb{F}_{q^2}(X)) = 4g(H) - 4g(X).$$

- $\mathrm{Ker}(\tau + i \cdot id_V)$: The last eigenspace is generated by the vectors $P \otimes a$ such that

$$P = (x_0 + r, y_0 + (x_0 + 1)r + s) \in E_{A,B},$$

with $x_0, y_0 \in \mathbb{F}_{q^2}(X)$. Using the equation of $E_{A,B}$, this means that $(x_0, y_0) \in E(\mathbb{F}_{q^2}(X))$. Reasoning as before shows

$$\dim_{\mathbb{Q}} \mathrm{Ker}(\tau + i \cdot id_V) = 4g(X).$$

The maximality/minimality assumption on C and E implies $\dim_{\mathbb{Q}} V = 4g(C)$, hence one concludes

$$4g(C) = 2\mathrm{rank}\, E_{A,B}(\mathbb{F}_{q^2}(X)) + 4g(H) - 4g(X) + 4g(X),$$

finishing the proof of Theorem 1.

5. Genera of the Curves C and H

To make the result in Theorem 1 more explicit, we review some results on the genus of the curves considered, in the special case that $X = \mathbb{P}^1$. Then $\mathbb{F}_q(X)$ equals the rational function field $\mathbb{F}_q(t)$. We consider the case that $A = A(t), B = B(t)$ are polynomials in t. In particular, this implies that the elliptic surface over $\mathbb{P}^1$ defined by $E_{A,B}$ has only one singular fiber (namely at $t = \infty$).

The change of variables ($\tilde{r} = r + c, \tilde{s} = s + cr + d$) with $c, d \in \mathbb{F}_q[t]$ brings the system

$$\begin{cases} r^2 + r = A(t), \\ s^2 + s = rA(t) + B(t) \end{cases}$$

in the form

$$\begin{cases} \tilde{r}^2 + \tilde{r} = \tilde{A}(t), \\ \tilde{s}^2 + \tilde{s} = \tilde{r}\tilde{A}(t) + \tilde{B}(t), \end{cases}$$

where $\tilde{A}(t) = A(t) + c^2 + c$ and $\tilde{B}(t) = B(t) + (c^2 + c)A(t) + c^3 + c^2 + d^2 + d$. As a consequence, for the properties of the curves C, H over $\mathbb{F}_q$, without loss of generality one may assume that $A(t) + A(0), B(t) + B(0) \in t\overline{\mathbb{F}}_q[t^2]$ (in particular, this results in polynomials of odd degree). We omit a proof of the following well-known result.

Proposition 2. *If $A(t) \in \mathbb{F}_q[t]$ has odd degree, then the genus of the hyperelliptic curve*

$$H : r^2 + r = A(t)$$

in characteristic 2 *is* $g(H) = \frac{\deg A - 1}{2}$.

Considering the curve C, the result is as follows. For convenience, a sketch of the proof is added.

Proposition 3. *If* $\deg A(t)$ *and* $\deg B(t)$ *are odd, then the genus of the curve C is*

$$g(C) = \max\left\{\frac{5 \cdot \deg A - 3}{2}, \frac{2 \cdot \deg B + \deg A - 3}{2}\right\}.$$

Proof. We use the notations as in [11, Proposition 3.7.8] and some Artin–Schreier theory for our wildly ramified field extensions

$$\begin{array}{c} F' = \overline{\mathbb{F}}_q(t, r, s), \\ \Big| \\ F = \overline{\mathbb{F}}_q(t, r), \\ \Big| \\ K = \overline{\mathbb{F}}_q(t). \end{array}$$

There is only one place (called P_∞ here) in $\mathbb{P}_F$ lying over $P_{1/t}$ and above each finite place $P_{t-\alpha} \in \mathbb{P}_K$, where $\alpha \in \overline{\mathbb{F}}_q$, we have two places in $\mathbb{P}_F$, denoted by P_α^0 and P_α^1.

The rational function $w = A(t)$ viewed as an element of $\overline{\mathbb{F}}_q(t, r)$ has the divisor

$$\operatorname{div}(w) = \sum m_\alpha P_\alpha^0 + \sum m_\alpha P_\alpha^1 - 2(\deg A) P_\infty.$$

Using

$$\operatorname{div}(r) = \sum m_\alpha P_\alpha^0 - (\deg A) P_\infty,$$

it follows that

$$\operatorname{div}(rA(t)) = 2 \sum m_\alpha P_\alpha^0 + \sum m_\alpha P_\alpha^1 - 3(\deg A) P_\infty.$$

The polynomial $B(t)$ has its only pole in P_∞. Therefore, the only possible ramified place at the field extension F'/F is P_∞. We now need to find the smallest odd value of $v_{P_\infty}(rA(t) + B(t) + z^2 + z)$, with $z \in F$. For that, choose a local parameter u at P_∞ and write

$$r = u^{-\deg A} \cdot \eta,$$

with $v_{P_\infty}(\eta) = 0$. Since $\deg A \not\equiv 0 \pmod 2$, working in the completed local ring at P_∞ one obtains v such that $\eta = v^{-\deg A}$. Therefore, defining $\pi = u \cdot v$, one obtains

$$r = \pi^{-\deg A}.$$

Since $v_{P_\infty}(t) = -2$, write

$$t = a_{-2}\pi^{-2} + a_{-1}\pi^{-1} + \cdots.$$

Let

$$A(t) = \alpha_d t^d + \alpha_{d-1} t^{d-1} + \cdots + \alpha_0.$$

In terms of π, the equation $r^2 + r = A(t)$ yields

$$\begin{aligned} \pi^{-2d} + \pi^{-d} &= \alpha_d (a_{-2}\pi^{-2} + a_{-1}\pi^{-1} + \cdots)^d \\ &\quad + \alpha_{d-1}(a_{-2}\pi^{-2} + a_{-1}\pi^{-1} + \cdots)^{d-1} + \cdots + \alpha_0 \\ &= \alpha_d a_{-2}^d \pi^{-2d} + \alpha_d a_{-2}^{d-1} a_{-1} \pi^{-2d+1} + \sum_{\alpha=2}^{\infty} c_\alpha \pi^{-2d+\alpha}, \end{aligned}$$

where

$$\begin{aligned} c_\alpha &= \alpha_d a_{-2}^{d-1} a_{\alpha-2} + \sum b_{\alpha,i} a_{-2}^{i_{-2}} a_{-1}^{i_{-1}} \cdots a_{\alpha-3}^{i_{\alpha-3}} \\ &\qquad \text{with } (-2)i_{-2} + (-1)i_{-1} + \cdots + (\alpha - 3) i_{\alpha-3} = -2d + \alpha, \end{aligned}$$

where $b_{\alpha,i}$ involves the coefficients of $A(t)$ and binomial coefficients.

This implies

$$\alpha_d a_{-2}^d = 1; \quad a_{-1} = 0; \quad \text{and} \quad c_\alpha = 0 \quad \text{if } \alpha \neq d.$$

The latter condition gives an expression of $a_{\alpha-2}$ in terms of $a_{-2}, \ldots, a_{\alpha-3}$. If α is odd, we know that any monomial on the expression of c_α has at least one coefficient of odd index. Starting from $a_{-1} = 0$ and using $c_\alpha = 0$ if $\alpha \neq d$, we obtain, inductively,

$$a_{-1} = a_1 = \cdots = a_{d-4} = 0 \quad \text{and} \quad \alpha_d a_{-2}^{d-1} a_{d-2} = 1.$$

Therefore,

$$t = a_{-2}\pi^{-2} + a_0 + \cdots + a_{d-2}\pi^{d-2} + \cdots.$$

Writing

$$B(t) = \beta_{d'} t^{d'} + \beta_{d'-1} t^{d'-1} + \cdots + \beta_0$$

(of odd degree d') and using the expansion of t obtained above, we conclude that the smallest odd power of π appearing on $B(t)$ is

$$\beta_{d'} a_{-2}^{d'-1} a_{d-2} \pi^{-(2d'-d)}.$$

Hence, as above, one finds $z \in F$ such that $v_{P_\infty}(B(t) + z^2 + z) = 2\deg B - \deg A$. Then,

$$\begin{aligned} -v_{P_\infty}(r \cdot A(t) + B(t) + z^2 + z) &= \max\{v_{P_\infty}(r \cdot A(t)), v_{P_\infty}(B(t) + z^2 + z)\} \\ &= \max\{3 \cdot \deg A, 2 \cdot \deg B - \deg A\} =: m_{P_\infty}. \end{aligned}$$

The genus formula for an Artin–Schreier extension now gives

$$\begin{aligned} g(C) = 2g(H) + \frac{m_{P_\infty} - 1}{2} &= \frac{2\deg A + m_{P_\infty} - 3}{2} \\ &= \max\left\{\frac{5\deg A - 3}{2}, \frac{2\deg B + \deg A - 3}{2}\right\}. \end{aligned}$$ □

6. Examples

Here, some examples defined over $\mathbb{F}_q$ are presented where the conditions in Theorem 1 are satisfied. We always consider $\mathbb{F}_{16} \subseteq \mathbb{F}_q$. In particular, q is a square.

6.1. *A genus* 6 *example*

A simple and well-known case of a maximal curve over $\mathbb{F}_{16}$ is the plane quintic

$$C : y^4 + y = x^5.$$

This curve has genus $(5-1)(5-2)/2 = 6$. An automorphism σ of order 4 is given by

$$\sigma : (x, y) \mapsto (x + c, y + c^4 x + c),$$

with $c \in \mathbb{F}_{16}$ satisfying $c^4 + c^3 + 1 = 0$. Then $c^5 \in \mathbb{F}_4^\times$ has order 3, and

$$\sigma^2 : (x, y) \mapsto (x, y + c^5).$$

One observes that $\eta = c^5y^2 + c^{10}y$ and $\xi = c^2x$ generate the field of invariants in the function field $\mathbb{F}_{16}(C) = \mathbb{F}_{16}(x, y)$ under σ^2, with the relation

$$\eta^2 + \eta = \xi^5.$$

The action of σ on this subfield $\mathbb{F}_{16}(\xi, \eta) = \mathbb{F}_{16}(C/\langle\sigma^2\rangle)$ is given as

$$\sigma : (\xi, \eta) \mapsto (\xi + c^3, \eta + c^9\xi^2 + c^{12}\xi + c^{10}),$$

and here, the convenient generators for the subfield of elements fixed by σ acting on $\mathbb{F}_{16}(\xi, \eta)$ are

$$u := c^4\xi \cdot \sigma(\xi) \quad \text{and} \quad v := c^{10}\eta \cdot \sigma(\eta).$$

Replacing u by $u_1 = u + 1$ and v by $w := u_1 + (v + 1)/u_1$ results in new generators, satisfying $w^2 + w = u_1^3 + u_1$, the equation of the elliptic curve E considered throughout this paper.

To conclude, this example results in a case

$$(E \times C)/\langle\iota \times \sigma\rangle \to X = C/\langle\sigma\rangle = E$$

over $\mathbb{F}_{16}$ with the base curve $X = E$ of genus 1, and with the Mordell–Weil rank

$$2g(C) - 2g(C/\langle\sigma^2\rangle) = 12 - 4 = 8.$$

6.2. *Curves* $C : y^2 + y = x^{q+1}$

In this subsection, we prove the following.

Proposition 4. *Let $q = 2^{2n}$ with n odd. Then, for any $b_0, c \in \mathbb{F}_{q^2}$ such that*

$$b_0^2 + b_0 = c^{q+1} \quad \text{and} \quad \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(c^{q+1}) = 1,$$

the elliptic curve

$$\begin{aligned}\eta^2 + \eta = \xi^3 &+ \left(\frac{t}{c^2}\right)\xi^2 + \left(\frac{t + c^2}{c^2}\right)\xi + \frac{t^2}{c^4} \\ &+ t\left(c^{q-1} + \left(b_0 + \sum_{j=0}^{2n-2}\left(\frac{t}{c^2}\right)^{2^j}(b_0 + 1 + b_0^{2^{j+1}})\right)^2 \Big/ c\right)\end{aligned}$$

has rank q over $\mathbb{F}_{q^2}(t)$.

Proof. Consider the curve

$$C : y^2 + y = x^{q+1}.$$

For convenience, we recall the elementary argument showing that $C/\mathbb{F}_{q^2}$ is maximal. Note that Proposition 2 implies that the genus $g(C)$ of C equals $q/2$. For any $\alpha \in \mathbb{F}_{q^2}$, the norm $\nu := \alpha^{q+1}$ is in $\mathbb{F}_q$. Hence, the separable (since the characteristic is 2) polynomial $T^2 + T + \nu$ has two zeros $\beta \in \mathbb{F}_{q^2}$ and this yields $2q^2$ points $(\alpha, \beta) \in C(\mathbb{F}_{q^2})$. Together with the unique rational point at infinity, one concludes

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

Note that this works for any $q = 2^m$. The condition $q = 4^n$ with n odd in the assumptions of the proposition assures that the maximality/minimality of C and of $E : y^2 + y = x^3 + x$ are aligned.

We now show that $\mathbb{F}_{q^2}(C)$ can be seen as a cyclic degree 4 extension of $\mathbb{F}_{q^2}(t)$.

It is known from [15, Remarks 3.3 and 4.2] that the order 4 automorphisms of C are given by

$$\varphi_c : (x, y) \mapsto (x + c, y + b_0 + B(x)),$$

where $(c, b_0) \in C$, $B(x) = \sum_{i=0}^{2n-1} (c^q x)^{2^i}$ and $B(c) = 1$. For any such φ_c, one has

$$\varphi_c^2 : (x, y) \mapsto (x, y + 1),$$

so φ_c^2 is the hyperelliptic involution on C.

Note that our assumption $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(c^{q+1}) = 1$ for $c \in \mathbb{F}_{q^2}$ is satisfied for precisely $q(q+1)/2$ elements c, as shown below from observing the composition of surjective maps

$$\mathbb{F}_{q^2} \xrightarrow{\text{Norm}} \mathbb{F}_q \xrightarrow{\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}} \mathbb{F}_2.$$

The condition on c is equivalent to the statement that the point $(c, b_0) \in C(\mathbb{F}_{q^2})$ satisfies $b_0 \in \mathbb{F}_{q^2} \backslash \mathbb{F}_q$. Fix such (c, b_0). By definition, $B(c) = \sum_{i=0}^{2n-1} (c^q c)^{2^i} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_2}(c^{q+1}) = 1$. Hence, φ_c is an order 4 automorphism defined over $\mathbb{F}_{q^2}$. The field of invariants in $\mathbb{F}_{q^2}(C) = \mathbb{F}_{q^2}(x, y)$ under φ_c^2 is $\mathbb{F}_{q^2}(x)$, and the action of φ_c on $\mathbb{F}_{q^2}(x)$ is given by $x \mapsto x + c$. As a result, $t := x^2 + cx$ generates the field of invariants under φ_c in $\mathbb{F}_{q^2}(C)$. Denoting $r := \frac{x}{c}$, one realizes C as

$$C : \begin{cases} r^2 + r = \dfrac{t}{c^2}, \\[2ex] y^2 + y = (c \cdot r)^{q+1}. \end{cases}$$

Following the proof of [1, Theorem 3] now brings $\mathbb{F}_{q^2}(C)$ in Artin and Schreier's standard form of a cyclic degree 4 extension of $\mathbb{F}_{q^2}(t)$ described on p. 3. In fact, starting from $r^2 = r + \frac{t}{c^2}$ and proceeding by induction shows that

$$r^{2^i} = r + \frac{t}{c^2} + \left(\frac{t}{c^2}\right)^2 + \cdots + \left(\frac{t}{c^2}\right)^{2^{i-1}}$$

and

$$(c \cdot r)^{q+1} = c^{q-1}t + c^{q+1}\left(1 + \left(\frac{t}{c^2}\right) + \left(\frac{t}{c^2}\right)^2 + \cdots + \left(\frac{t}{c^2}\right)^{q/2}\right) r.$$

Using $c^{q+1} = b_0 + b_0^2$, one writes

$$\begin{aligned}\varphi_c(y) &= y + b_0 + B(c\cdot r)\\ &= y + (b_0 + b_0^q)r\\ &\quad + \underbrace{b_0 + \frac{t}{c^2}(b_0^2 + b_0^q) + \left(\frac{t}{c^2}\right)^2 (b_0^4 + b_0^q) + \cdots + \left(\frac{t}{c^2}\right)^{q/4} (b_0^{q/2} + b_0^q)}_{D}.\end{aligned}$$

Since $\varphi_c^2(y) = y+1$, one concludes that $b_0 + b_0^q = 1$. Now, defining $s := y + D\cdot r$, one has $\varphi_c(s) = s + r$ and

$$\begin{aligned}s^2 + s &= y^2 + y + D^2\cdot r^2 + D\cdot r\\ &= c^{q-1}t + c^{q+1}\left(1 + \left(\frac{t}{c^2}\right) + \left(\frac{t}{c^2}\right)^2 + \cdots + \left(\frac{t}{c^2}\right)^{q/2}\right) r + D^2\left(r + \frac{t}{c}\right) + D\cdot r\\ &= \underbrace{t\left(c^{q-1} + \frac{D^2}{c}\right) + \underbrace{\left[c^{q+1}\left(1 + \left(\frac{t}{c^2}\right) + \left(\frac{t}{c^2}\right)^2 + \cdots + \left(\frac{t}{c^2}\right)^{q/2}\right) + D^2 + D\right]}_{E} r}_{\psi(r)}.\end{aligned}$$

Finally, note that

$$\psi(r+1) = \psi(\varphi_c(r)) = \varphi_c(\psi(r)) = \varphi_c(s^2+s) = (s+r)^2 + (s+r) = \psi(r) + \frac{t}{c^2}.$$

Since ψ is an expression of degree 1 in r, $\psi(r+1) - \psi(r)$ is the leading coefficient, namely E, so one obtains

$$s^2 + s = r\cdot\left(\frac{t}{c^2}\right) + t\left(c^{q-1} + \frac{D^2}{c}\right).$$

So, an Artin–Schreier standard form for C is

$$C : \begin{cases} r^2 + r = \dfrac{t}{c^2},\\[2ex] s^2 + s = r\dfrac{t}{c^2} + t\left(c^{q-1} + \left(b_0 + \displaystyle\sum_{j=0}^{2n-2}\left(\frac{t}{c^2}\right)^{2^j}(b_0 + 1 + b_0^{2^{j+1}})\right)^2 \Big/ c\right).\end{cases}$$

The proof of the proposition is now an immediate application of Theorem 1, using that the (hyperelliptic) curve C has genus $q/2$ and the intermediate curve in this case is the x-line, of genus 0. □

Corollary 5. *Given any natural number M, there is a power of 2 denoted q,, and an elliptic curve defined over $\mathbb{F}_{q^2}(t)$ such that its rank over $\mathbb{F}_{q^2}(t)$ equals $q > M$.*

Remark 6. It is possible to replace the curve $y^2 + y = x^{q+1}$ in this subsection by a more general curve $y^2 + y = xR(x)$, where $R(x)$ is an additive polynomial, which is maximal (respectively, minimal) over odd (respectively, even) degree extensions of $\mathbb{F}_{16}$. This replacement will provide new families of elliptic curves defined over the function fields of even characteristic having arbitrarily large Mordell–Weil rank.

This discussion will be presented in João Paulo Guardieiro's Ph.D. thesis, as well as the analogous results of this paper in the additional case of function fields of characteristic 3 obtained from cubic twists of a supersingular elliptic curve defined over $\mathbb{F}_3$.

6.3. *Trace examples*

For any positive integer m, put $\mathrm{Tr}(t) := t + t^2 + \cdots + t^{2^{m-1}}$ so that in particular, $\alpha \mapsto \mathrm{Tr}(\alpha)$ is the trace function $\mathrm{Tr}_{\mathbb{F}_{2^m}/\mathbb{F}_2} : \mathbb{F}_{2^m} \to \mathbb{F}_2$.

Proposition 7. *Let $q = 2^m$ with m odd. Then,*

$$E_{\mathrm{Tr}(t),0} : \eta^2 + \eta = \xi^3 + \mathrm{Tr}(t)\xi^2 + (\mathrm{Tr}(t)+1)\xi + \mathrm{Tr}(t)^2$$

has rank q over $\mathbb{F}_{q^4}(t)$.

Proof. Note that, for odd m, the curve

$$H : r^2 + r = \mathrm{Tr}(t) = t + t^2 + \cdots + t^{2^{m-1}}$$

is rational; explicitly, it is parameterized by

$$(t, r) = (x^2 + x,\ x + x^2 + \cdots + x^{2^{m-1}}).$$

Consider the Artin–Schreier covering of H given by

$$C : \begin{cases} r^2 + r = \mathrm{Tr}(t), \\ s^2 + s = r \cdot \mathrm{Tr}(t). \end{cases}$$

Using the parametrization, the genus and the number of points of C can be studied from the resulting equation:

$$\begin{aligned} s^2 + s &= (x + x^2 + \cdots + x^{2^{m-1}}) \cdot \mathrm{Tr}(x^2 + x) \\ &= (x + x^2 + \cdots + x^{2^{m-1}}) \cdot (x^{2^m} + x) \\ &= \sum_{n=0}^{m-1} (x \cdot x^{2^n} + x^{2^m} \cdot x^{2^n}). \end{aligned}$$

Since $x^{2^n} \cdot x^{2^m} \equiv x \cdot x^{2^{m-n}} \bmod \wp(\mathbb{F}_2[x])$ with as before $\wp$ the Artin–Schreier operator $f \mapsto f^2 + f$, one may replace $x^{2^n} \cdot x^{2^m}$ by $x \cdot x^{2^{m-n}}$ in the latter expression. As a consequence, the curve C is isomorphic to the one with the equation

$$\begin{aligned} s^2 + s &= (x \cdot x^{2^m} + x \cdot x^{2^{m-1}} + \cdots + x \cdot x^2) + x(x + x^2 + \cdots + x^{2^{m-1}}) \\ &= x(x^{2^m} + x). \end{aligned}$$

Hence, the genus of C equals $2^{m-1} = q/2$. Maximality over $\mathbb{F}_{q^4}$ follows from the results of [4]. Theorem 1 now finishes the proof. $\square$

Observe that the examples in Secs. 6.2 and 6.3 involve only hyperelliptic curves. We have not found any non-hyperelliptic curve C with $\sigma \in \mathrm{Aut}_{\mathbb{F}_{q^2}}(C)$ for large q satisfying both maximality over $\mathbb{F}_{q^2}$ and $C/\langle\sigma\rangle \cong \mathbb{P}^1$. Since a potential example satisfies

$$q^2 + 1 + 2g(C)q = \#C(\mathbb{F}_{q^2}) \leq 4 \cdot \#\mathbb{P}^1(\mathbb{F}_{q^2}),$$

it would necessarily have $g(C) < 3(q^2+1)/(2q)$.

7. The Mordell–Weil Rank via the Shioda–Tate Formula

In what follows, we determine the geometric Mordell–Weil rank of the elliptic curve $E_{A,B}$, namely its rank over $\overline{\mathbb{F}}_q(t)$. This is a direct application of the Shioda–Tate formula and hence depends only on the type(s) of singular fiber(s) of $E_{A,B}$ and the Picard number of the associated elliptic surface. The former depends only on the degrees of $A(t)$ and $B(t)$ and is described in Proposition 8, while the latter is equal to the second Betti number, since $E_{A,B}$ is supersingular. We conclude the section by comparing the geometric Mordell–Weil rank with that over $\mathbb{F}_{q^2}$ obtained in Sec. 2.

Proposition 8. *Let $A, B \in \mathbb{F}_q[t]$ be the polynomials of odd degree. Consider the elliptic surface $E_{A,B}$ given in* (2). *The only singular fiber of this surface is at infinity, and its type can be found in the following table*:

Condition on the degrees	*Fiber type*
$3\deg A(t) \geq \deg B(t)$	I_m^*, $m = 2 \cdot \min\{\deg A(t), 3\deg A(t) - \deg B(t)\}$
$3\deg A(t) < \deg B(t) \equiv 1 \pmod 6$	II^*
$3\deg A(t) < \deg B(t) \equiv 3 \pmod 6$	I_0^*
$3\deg A(t) < \deg B(t) \equiv 5 \pmod 6$	II

Proof. Consider

$$E_{A,B} : \eta^2 + \eta = \xi^3 + A(t)\xi^2 + (A(t)+1)\xi + \underbrace{A(t)^2 + B(t)}_{a_6(t)}.$$

The discriminant of this equation is $\Delta \equiv 1$. Therefore, the only possible singular fiber is at infinity. To study its behavior, we denote by n the Euler number of the associated elliptic surface, i.e. the smallest integer such that

$$\deg A(t) \leq 2n \quad \text{and} \quad \deg(A(t)^2 + B(t)) \leq 6n.$$

More precisely, we have

$$n = \begin{cases} \dfrac{\deg A(t) + 1}{2} & \text{if } \deg B(t) \leq 3 \cdot \deg A(t), \\[2ex] \dfrac{\deg B(t) + m}{6} & \text{if } \deg B(t) > 3 \cdot \deg A(t) \text{ and } \deg B(t) \equiv -m \pmod 6. \end{cases}$$

Let

$$x = \frac{\xi}{t^{2n}}, \quad y = \frac{\eta}{t^{3n}} \quad \text{and} \quad s = \frac{1}{t},$$

and divide the equation of $E_{A,B}$ by t^{6n}. We obtain

$$y^2 + s^{3n}y = x^3 + s^{2n-\deg A(t)}\tilde{A}(s)x^2 + s^{4n-\deg A(t)}\overline{A}(s)x + s^{6n-\deg a_6(t)}\tilde{a}_6(s),$$

where

$$s \nmid \tilde{A}(s), \overline{A}(s), \tilde{a}_6(s).$$

Then, the quantities as in [10, Sec. III.1] are as follows:

$$b_2 = b_4 = 0, \quad b_6 = s^{6n}, \quad b_8 = s^{8n-\deg A(t)}\tilde{A}(s) + s^{8n-2\deg A(t)}\overline{A}(s).$$

This puts one in a position to apply Tate's algorithm [13] to find the type of the fiber at infinity (which is now the fiber at $s = 0$). Since $b_2 = 0$, the singular fiber is of additive type. If $3\deg A(t) \geq \deg B(t)$, then, following Tate's algorithm, one shows that the fiber is of type I_m^*. Otherwise, the specific type depends on the congruence class of the degree of $B(t)$ modulo 6. □

Remark 9. The phenomenon described in Proposition 8, namely the presence of a unique singular fiber in a nontrivial elliptic fibration, is particular to fields of characteristics 2 and 3 and described, for instance, in [6] for the rational elliptic surfaces with Mordell–Weil rank zero. More surprisingly, Proposition 8 shows that there are examples of arbitrarily high Mordell–Weil rank such that all fibers are irreducible and only one of them is singular. Indeed, the ones given by an equation of the form $E_{A,B}$ as in (2) with $3\deg A(t) < \deg B(t)$ and $\deg B(t) \equiv 5 \mod 6$ are of such type.

As a corollary of the proof of Proposition 8, we obtain the following.

Corollary 10. *The second Betti number of the elliptic surface $E_{A,B}$ is*

$$b_2 = \begin{cases} 12\left\lceil \dfrac{\deg B(t)}{6} \right\rceil - 2 & \text{if } \deg B(t) > 3\deg A(t), \\[2ex] 12\left\lceil \dfrac{\deg A(t)}{2} \right\rceil - 2 & \text{if } \deg B(t) \leq 3\deg A(t). \end{cases} \tag{4}$$

Proof. This follows from [7, Sec. 6.10] for elliptic fibrations with rational base combined with the proof of Proposition 8. □

Theorem 11. *Let r be the geometric Mordell–Weil rank of $E_{A,B}$. Then,*

$$r = -2 + \begin{cases} 2\deg B(t) & \text{if } \deg B(t) > 3\deg A(t), \\ 6\deg A(t) - 2\cdot\min\{\deg A(t), & \\ \qquad 3\deg A(t) - \deg B(t)\} & \text{if } \deg B(t) \leq 3\deg A(t). \end{cases} \tag{5}$$

Proof. Since $E_{A,B}$ is supersingular, the rank of the Néron–Severi group ρ of the elliptic surface associated to $E_{A,B}$ is equal to the second Betti number of the surface, b_2. This combined with the information about the singular fiber of $E_{A,B}$ given in Proposition 8 puts us in a position to apply the Shioda–Tate formula (see [7, Corollary 6.13]) and obtain the desired equality for r. □

We can finally interpret the results of this section in the light of the previous ones.

Corollary 12. *If the curves C and E, as in Sec.* 2, *are both maximal or minimal over $\mathbb{F}_{q^2}$, then the geometric Mordell–Weil rank of $E_{A,B}$ is attained over $\mathbb{F}_{q^2}$.*

Proof. This is a combination of Theorems 1 and 11 and Proposition 3. □

Acknowledgments

This work was developed during the stay of João Paulo Guardieiro at the Bernoulli Institute of the Rijksuniversiteit Groningen. He is happy to thank the institute for its hospitality.

Herivelto Borges was supported by CNPq (Brazil), Grants 406377/2021-9 and 310194/2022-9, and by FAPESP (Brazil), Grant 2022/15301-5. João Paulo Guardieiro was supported by CNPq (Brazil), Grant 140589/2021-0, and by CAPES (Brazil), Finance Code 001. Cecília Salgado was partially supported by the NWO-XL "Rational Points: New Dimensions" Consortium Grant.

ORCID

Herivelto Borges https://orcid.org/0000-0002-8100-3486
João Paulo Guardieiro https://orcid.org/0000-0003-2831-9294
Cecília Salgado https://orcid.org/0000-0002-5650-6823
Jaap Top https://orcid.org/0000-0002-5265-7608

References

[1] E. Artin and O. Schreier, Eine Kennzeichnung der reell abgeschlossenen Körper, *Abh. Math. Semin. Univ. Hambg.* **5**(1) (1927) 225–231.
[2] S. Bootsma, S. Tafazolian and J. Top, Maximal curves and Tate–Shafarevich results for quartic and sextic twists, *Finite Fields Appl.* **91** (2023) 102256.
[3] J. S. Chahal, A. Soomro and J. Top, A supplement to Manin's proof of the Hasse inequality, *Rocky Mountain J. Math.* **44**(5) (2014) 1457–1470.
[4] R. S. Coulter, The number of rational points of a class of Artin–Schreier curves, *Finite Fields Appl.* **8**(4) (2002) 397–413.
[5] N. D. Elkies, Mordell–Weil lattices in characteristic 2: I: Construction and first properties, *Int. Math. Res. Not. IMRN* **1994**(8) (1994) 343–361.
[6] W. E. Lang, Extremal rational elliptic surfaces in characteristic p: II: Surfaces with three or fewer singular fibres, *Ark. Mat.* **32**(2) (1994) 423–448.

[7] M. Schuett and T. Shioda, Elliptic surfaces, preprint, arXiv:0907.0298 [math.AG] (2009).
[8] M. Schütt and T. Shioda, *Mordell–Weil Lattices*, A Series of Modern Surveys in Mathematics (MATHE3), Vol. 70 (Springer, 2019).
[9] T. Shioda, Mordell–Weil lattices and sphere packings, *Amer. J. Math.* **113**(5) (1991) 931–948.
[10] J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, Vol. 106 (Springer, 2009).
[11] H. Stichtenoth, *Algebraic Function Fields and Codes*, Graduate Texts in Mathematics, Vol. 254 (Springer Science & Business Media, 2009).
[12] J. Tate, Endomorphisms of abelian varieties over finite fields, *Invent. Math.* **2** (1966) 134–144.
[13] J. Tate, Algorithm for determining the type of a singular fiber in an elliptic pencil, in *Modular Functions of One Variable IV*, Lecture Notes in Mathematics, Vol. 476 (Springer, 2006), pp. 33–52.
[14] J. T. Tate and I. R. Šafarevič, The rank of elliptic curves, *Dokl. Akad. Nauk SSSR* **175** (1967) 770–773.
[15] G. van der Geer and M. van der Vlugt, Reed-Muller codes and supersingular curves: I, *Compos. Math.* **84**(3) (1992) 333–367.