Weierstrass semigroups and automorphism group of a maximal curve with the third largest genus

Beelen, Peter; Montanucci, Maria; Vicino, Lara

Published in:
Finite Fields and Their Applications

Link to article, DOI:
10.1016/j.ffa.2023.102300

Publication date:
2023

Document Version
Publisher's PDF, also known as Version of record

Citation (APA):
Beelen, P., Montanucci, M., & Vicino, L. (2023). Weierstrass semigroups and automorphism group of a maximal curve with the third largest genus. *Finite Fields and Their Applications*, *92*, Article 102300. https://doi.org/10.1016/j.ffa.2023.102300

Finite Fields and Their Applications 92 (2023) 102300

Contents lists available at ScienceDirect

Finite Fields and Their Applications

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

Weierstrass semigroups and automorphism group of a maximal curve with the third largest genus

Peter Beelen, Maria Montanucci [*], Lara Vicino

Department of Applied Mathematics and Computer Science, Technical University of Denmark, Kongens Lyngby 2800, Denmark

ARTICLE INFO

Article history:
Received 31 March 2023
Received in revised form 30 June 2023
Accepted 30 August 2023
Available online xxxx
Communicated by Gary L. Mullen

MSC:
primary 11G20
secondary 11R58, 14H05, 14H55

Keywords:
Maximal curve
Weierstrass semigroup
Weierstrass points

ABSTRACT

In this article we explicitly determine the Weierstrass semigroup at any point and the full automorphism group of a known $\mathbb{F}_{q^2}$-maximal curve $\mathcal{X}_3$ having the third largest genus. This curve arises as a Galois subcover of the Hermitian curve, and its uniqueness (with respect to the value of its genus) is a well-known open problem. Knowing the Weierstrass semigroups may provide a key towards solving this problem. Surprisingly enough $\mathcal{X}_3$ has many different types of Weierstrass semigroups and the set of its Weierstrass points is much richer than its set of $\mathbb{F}_{q^2}$-rational points. This makes the curve $\mathcal{X}_3$ the first explicitly known maximal curve having non-rational Weierstrass points. We show that a similar exceptional behaviour does not occur in terms of automorphisms, that is, $\text{Aut}(\mathcal{X}_3)$ is exactly the automorphism group inherited from the Hermitian curve, apart from small values of q.

[*] Corresponding author.
E-mail addresses: pabe@dtu.dk (P. Beelen), marimo@dtu.dk (M. Montanucci), lavi@dtu.dk (L. Vicino).

https://doi.org/10.1016/j.ffa.2023.102300

1. Introduction

An $\mathbb{F}_{q^2}$-maximal curve $\mathcal{X}$ of genus $g(\mathcal{X})$ is a projective, geometrically irreducible, non-singular algebraic curve defined over $\mathbb{F}_{q^2}$ such that the number $|\mathcal{X}(\mathbb{F}_{q^2})|$ of its $\mathbb{F}_{q^2}$-rational points attains the Hasse-Weil upper bound, namely

$$|\mathcal{X}(\mathbb{F}_{q^2})| = q^2 + 1 + 2g(\mathcal{X})q.$$

$\mathbb{F}_{q^2}$-maximal curves and especially those with large genus have been intensively investigated during the last decades also in connection with coding theory and cryptography based on Goppa's method, see e.g. [13,26].

It is well known that the genus $g(\mathcal{X})$ of an $\mathbb{F}_{q^2}$-maximal curve $\mathcal{X}$ satisfies $g(\mathcal{X}) \leq q(q-1)/2 =: g_1$, see [17], and that $g(\mathcal{X}) = g_1$ if and only if $\mathcal{X}$ is $\mathbb{F}_{q^2}$-isomorphic to the Hermitian curve

$$\mathcal{H} : x^q + x = y^{q+1},$$

see [22]. In [8] it is proven that either $g(\mathcal{X}) \leq \lfloor (q-1)^2/4 \rfloor =: g_2$, or $g(\mathcal{X}) = g_1$. For q odd, $g(\mathcal{X}) = g_2$ occurs if and only if $\mathcal{X}$ is $\mathbb{F}_{q^2}$-isomorphic to the non-singular model of the plane curve of equation

$$\mathcal{X}_2 : x^q + x = y^{\frac{q+1}{2}},$$

see [7, Theorem 3.1]. For q even, a similar (but weaker) result is obtained in [1]. Indeed the uniqueness of an $\mathbb{F}_{q^2}$-maximal curve of genus $g(\mathcal{X}) = g_2$ is ensured under the extra condition that the curve has a particular Weierstrass point. If the extra condition is met, then it is proven in [1] that $g(\mathcal{X}) = q(q-2)/4$ if and only if $\mathcal{X}$ is $\mathbb{F}_{q^2}$-isomorphic to the non-singular model of the plane curve of equation

$$\mathcal{Y}_2 : x^{\frac{q}{2}} + \cdots + x^2 + x = y^{q+1}.$$

The value of the third largest genus of an $\mathbb{F}_{q^2}$-maximal curve $\mathcal{X}$ has been computed in [20], where it is proven that either $g(\mathcal{X}) \leq \lfloor (q^2 - q + 4)/6 \rfloor =: g_3$, or $g(\mathcal{X}) = g_2$ or $g(\mathcal{X}) = g_1$. In [20, Remark 3.4] it is shown that $g(\mathcal{X}) \leq g_3$ is the best bound possible, as there exist $\mathbb{F}_{q^2}$-maximal curves of genus g_3, namely

- $\mathcal{X}_3 : x^{(q+1)/3} + x^{2(q+1)/3} + y^{q+1} = 0$, if $q \equiv 2 \pmod 3$;
- $\mathcal{Y}_3 : y^q - yx^{2(q-1)/3} + x^{(q-1)/3} = 0$, if $q \equiv 1 \pmod 3$; and
- $\mathcal{Z}_3 : y^q + y + (\sum_{i=1}^{t} x^{q/p^i})^2 = 0$, if $q = 3^t$.

More precisely, $\mathcal{X}_3, \mathcal{Y}_3$ and $\mathcal{Z}_3$ are the non-singular models of the plane curves given by these equations. All the examples above arise as degree 3 Galois subcovers of the

Hermitian curve $\mathcal{H}$. Understanding whether or not these curves are the only $\mathbb{F}_{q^2}$-maximal curves of genus g_3 is a well-known open problem.

In the proofs of the uniqueness (up to isomorphism) of $\mathbb{F}_{q^2}$-maximal curves of genus g_1 and g_2 from [22] and [8] the so-called Weierstrass semigroups and Weierstrass points played a crucial role. These objects occur also naturally in the study of algebraic-geometry (AG) codes [26], as the main ingredient to construct one-point AG codes.

Given a point P on an algebraic curve $\mathcal{X}$, the Weierstrass semigroup $H(P)$ is defined as the set of natural numbers n for which there exists a function f on $\mathcal{X}$ having pole divisor $(f)_\infty = nP$. According to the Weierstrass gap Theorem, see [23, Theorem 1.6.8], the set $G(P) := \mathbb{N} \setminus H(P)$ contains exactly $g(\mathcal{X})$ elements called gaps. The structure of $H(P)$ in general varies as $P \in \mathcal{X}$ varies. However, it is known that generically the semigroup $H(P)$ is the same, but that there can exist finitely many points of $\mathcal{X}$, called Weierstrass points, with a different set of gaps.

The intrinsic theoretical interest on these objects arises from Stöhr-Voloch theory [24], where (together with the so-called order sequence) Weierstrass semigroups and points are used to obtain characterizing properties of the curve. Apart from the two characterizations for g_1 and g_2 mentioned above, important characterization results using Weierstrass points, semigroups and automorphism groups can be found in [7], [9] (for the Suzuki curve) and [25] (for the Ree curve).

In order to provide similar tools for maximal curves of third largest genus, it is natural to wonder whether Weierstrass semigroups and points can be completely determined for maximal curves of genus g_3.

In this paper we compute the Weierstrass semigroup at every point of the curve $\mathcal{X}_3$ having third largest genus g_3 for $q \equiv 2 \pmod 3$, as well as its set of Weierstrass points and its full automorphism group.

In all known examples of maximal curves with large enough genus the set of Weierstrass points coincides with that of rational points, see e.g. [3–5,11]. To understand this behaviour previous investigations found sufficient conditions for a maximal curve to satisfy this property, see [10].

In this paper, we show on the contrary that the curve $\mathcal{X}_3$ has a quite large set of non-rational Weierstrass points and many different type of Weierstrass semigroups, providing the first known example with these features. The full automorphism group of $\mathcal{X}_3$ is also computed, as an application of the results mentioned above.

The paper is organized as follows. Section 2 provides the necessary preliminary results on algebraic curves, Weierstrass semigroups and the curve $\mathcal{X}_3$. Section 3 presents two families of special functions in $\mathbb{F}_{q^2}(\mathcal{X}_3)$ and their relations. These functions represent the main ingredient used to compute the Weierstrass semigroups $H(P)$ apart from a few special cases of P. Sections 4 and 5 are devoted to the proofs of the main theorems of the paper, namely the description of the Weierstrass semigroup at $\mathbb{F}_{q^2}$-rational and not $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}_3$, respectively. In Section 6 the full automorphism group of $\mathcal{X}_3$ is computed as an application of the obtained results on Weierstass semigroups of $\mathcal{X}_3$.

2. Preliminaries

In this section, we deal with the preliminary notions and results that will be needed throughout the paper. In the first subsection, we recall the definition of the curve $\mathcal{X}_3$ and we focus on some particular rational functions defined on it, computing their principal divisors. In the second subsection, we collect some preliminaries on regular differentials. In particular, we compute a canonical divisor and prove Corollary 2.24, that we will need in Sections 4 and 5.

2.1. The curve $\mathcal{X}_3$

Let q be a prime power such that $q \equiv 2 \pmod 3$ and define $m := \frac{q+1}{3}$. Let $\mathbb{F}_{q^2}$ be the finite field with q^2 elements and denote by p the characteristic of $\mathbb{F}_{q^2}$. As before, let $\mathcal{X}_3$ be the non-singular model of the plane curve with affine equation

$$y^{q+1} + x^{2m} + x^m = 0. \tag{2.1}$$

The function field $\mathbb{F}_{q^2}(\mathcal{X}_3)$ can be described as $\mathbb{F}_{q^2}(x, y)$, with $y^{q+1} + x^{2m} + x^m = 0$, and it is easy to see that $\mathbb{F}_{q^2}(\mathcal{X}_3)/\mathbb{F}_{q^2}(x)$ is a Kummer extension of degree $q + 1$.

Remark 2.2. The point $(0, 0)$ is a singular point of the curve defined by equation (2.1). Considering what we have just observed on the desingularization $\mathcal{X}_3$ and its function field, it is then easy to see that there are exactly m distinct places centered on $(0, 0)$ in $\mathbb{F}_{q^2}(\mathcal{X}_3)$, and we denote as $P_0^1, \dots, P_0^m$ the distinct points of $\mathcal{X}_3$ that are the centers of such places. The point at infinity of the plane curve is singular as well. Also for this point there are exactly m distinct places centered on it in $\mathbb{F}_{q^2}(\mathcal{X}_3)$. We denote by $P_\infty^1, \dots, P_\infty^m$ the distinct points of $\mathcal{X}_3$ that are the centers of these m places.

Consider the $\mathbb{F}_{q^2}$-model of the Hermitian curve $\mathcal{H}$ given by

$$\mathcal{H} : u^{q+1} + v^{q+1} + 1 = 0$$

and let $\mathbb{F}_{q^2}(\mathcal{H})$ be the function field of $\mathcal{H}$, that can be described as $\mathbb{F}_{q^2}(u, v)$, with $u^{q+1} + v^{q+1} + 1 = 0$. The Hermitian curve is a nonsingular plane curve of genus $g(\mathcal{H}) = q(q - 1)/2$. The curve $\mathcal{X}_3$ is $\mathbb{F}_{q^2}$-maximal of genus $g(\mathcal{X}_3) := \frac{q^2-q+4}{6}$ and it is $\mathbb{F}_{q^2}$-covered by the Hermitian curve $\mathcal{H}$ via a morphism φ of degree 3. More precisely, the pull-back map

$$\varphi^* : \mathbb{F}_{q^2}(\mathcal{X}_3) \longrightarrow \mathbb{F}_{q^2}(\mathcal{H})$$

defines a Galois extension $\mathbb{F}_{q^2}(\mathcal{H})/\mathbb{F}_{q^2}(\mathcal{X}_3)$ of degree 3, with $x := u^3$ and $y := uv$. In particular, the Galois group of the extension is generated by the automorphism

$$\tau : (u, v) \longmapsto (\zeta_3 u, \zeta_3^2 v), \tag{2.3}$$

where ζ_3 is a primitive cube root of unity in $\mathbb{F}_{q^2}$.

Remark 2.4. The extension $\mathbb{F}_{q^2}(\mathcal{H})/\mathbb{F}_{q^2}(\mathcal{X}_3)$ is unramified: indeed, by the Hurwitz genus formula, it holds

$$\deg \operatorname{Diff}(\mathbb{F}_{q^2}(\mathcal{H})/\mathbb{F}_{q^2}(\mathcal{X}_3)) = 2g(\mathcal{H}) - 2 - 3(2g(\mathcal{X}_3) - 2) = 0,$$

which means precisely that the extension $\mathbb{F}_{q^2}(\mathcal{H})/\mathbb{F}_{q^2}(\mathcal{X}_3)$ is unramified. As a consequence of this fact, if Q is a point of $\mathcal{H}$ lying over the point P of $\mathcal{X}_3$, then for any $f \in \mathbb{F}_{q^2}(\mathcal{X}_3)$, it holds that $v_Q(f) = v_P(f)$.

For convenience, we define $\mathcal{O}_0 := \{P_0^1, \ldots, P_0^m\}$ and $\mathcal{O}_\infty := \{P_\infty^1, \ldots, P_\infty^m\}$. Throughout the paper, we denote with $P_{(a,b)} \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2})$ a point of $\mathcal{X}_3$ not in the set of points $\mathcal{O}_0 \cup \mathcal{O}_\infty$, with (x, y)-coordinates (a, b). With this convention in mind, in particular, the x-coordinate a of such a point $P_{(a,b)}$ is nonzero. Analogously, we denote with $Q_{(A,B)} \in \mathcal{H}$ a point of $\mathcal{H}$ with (u, v)-coordinates (A, B) and not lying over any point of $\mathcal{X}_3$ in the set $\mathcal{O}_0 \cup \mathcal{O}_\infty$. The points in the set $\mathcal{O}_0 \cup \mathcal{O}_\infty$ turn out to lie in the same orbit under the action of the full automorphism group of $\mathcal{X}_3$. In fact, the orbit turns out to be given by:

$$\mathcal{O} := \mathcal{O}_0 \cup \mathcal{O}_\infty \cup \mathcal{O}_m, \tag{2.5}$$

where $\mathcal{O}_m := \{P_{(a,0)} \mid a^m + 1 = 0\}$. It will be convenient to establish some of these results already now, so that we will be able to determine the Weierstrass semigroups of points in this orbit efficiently. In Section 6, we will then continue the study of automorphisms on $\mathcal{X}_3$.

Lemma 2.6. *The automorphism group* $\operatorname{Aut}(\mathcal{X}_3)$ *contains a subgroup* G *of order* $2(q+1)^2$ *which is isomorphic to a semidirect product of an abelian group* A *of order* $(q+1)^2/3$ *and a symmetric group of order* 6*. More precisely,*

$$A := \{\theta_{\gamma,\delta}(x, y) = (\gamma x, \delta y) \mid \gamma^m = \delta^{q+1} = 1\},$$

while the symmetric group of order 6 *is generated by the involution* θ_2 *and the order* 3 *automorphism* θ_3 *given by*

$$\theta_2(x, y) = \left(\frac{1}{x}, \frac{y}{x}\right) \text{ and } \theta_3(x, y) = \left(\frac{y^3}{x^2}, \frac{y}{x}\right).$$

Proof. By direct computation it can be checked that $\langle A, \theta_2, \theta_3 \rangle$ is an automorphism group of $\mathcal{X}_3$, that is, all the maps presented in the lemma preserve the equation $y^{q+1} + x^m + x^{2m} = 0$. The group T generated by θ_2 and θ_3 is isomorphic to the symmetric group of order 6 as $\theta_2\theta_3\theta_2 = \theta_3^2$, by direct computation. Both θ_2 and θ_3 normalize A, since a direct computation shows $\theta_2\theta_{\gamma,\delta}\theta_2 = \theta_{\gamma^{-1},\delta\gamma^{-1}}$ and $\theta_3\theta_{\gamma,\delta}\theta_3^{-1} = \theta_{\gamma\delta^{-3},\gamma\delta^{-2}}$. Hence T normalizes A. Since T and A have trivial intersection, we hence obtain that $\langle A, T\rangle = A \rtimes T$. □

Next let us determine divisors of several elementary function in $\mathbb{F}_{q^2}(\mathcal{X}_3)$. We denote as D_∞ the divisor

$$D_\infty := \sum_{j=1}^{m} P_\infty^j. \tag{2.7}$$

Since $\mathcal{X}_3$ is $\mathbb{F}_{q^2}$-maximal, from the Fundamental Equation [15, Page xvii (ii)] it follows in particular that, for all $i = 1, \ldots, m$ and $P_{(a,b)} \in \mathcal{X}_3$, there exists a function $f_{P_{(a,b)},i} \in \mathbb{F}_{q^2}(\mathcal{X}_3)$ such that

$$(f_{P_{(a,b)},i}) = qP_{(a,b)} + \Phi(P_{(a,b)}) - (q+1)P_\infty^i. \tag{2.8}$$

Here Φ denotes the $\mathbb{F}_{q^2}$-Frobenius map. For a point $P_{(a,b)}$ of $\mathcal{X}_3$, we define the function

$$x_a := \frac{x-a}{a},$$

which, as we will see later, turns out to be a local parameter for $P_{(a,b)}$. Further, let $t_{P(a,b)}$ be the following function in $\mathbb{F}_{q^2}(\mathcal{X}_3)$

$$t_{P_{(a,b)}} := ma^{m-1}(2a^m+1)(x-a) + b^q(y-b), \tag{2.9}$$

and let $Q_{(A,B)}$ be a point of $\mathcal{H}$ lying over $P_{(a,b)}$. Note that $t_{P_{(a,b)}}$ is the function associated to the tangent line at (a, b) of the plane curve defined by equation (2.1).

With $\mathcal{O}$ defined as in equation (2.5), for $P_{(a,b)} \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \setminus \mathcal{O}$, we define

$$\alpha(P_{(a,b)}) := \frac{a^m}{1+a^m} = \frac{A^{q+1}}{1+A^{q+1}}. \tag{2.10}$$

As $1 - \alpha(P_{(a,b)}) = \frac{1}{1+a^m}$, in particular $1 - \alpha(P_{(a,b)}) \neq 0$ and we can define the following nonzero function in $\mathbb{F}_{q^2}(\mathcal{X}_3)$, that will be useful later:

$$f_0 := \frac{3(1-\alpha(P_{(a,b)}))}{A^{q+1}} t_{P_{(a,b)}} = (1-\alpha(P_{(a,b)}))\left(\frac{(2A^{q+1}+1)}{A^3}(x-a) + \frac{3B^q}{A}(y-b)\right), \tag{2.11}$$

where $A^3 = a$ and $AB = b$. Given a point $P_{(a,b)} \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \setminus \mathcal{O}$ and $Q_{(A,B)}$ a point of $\mathcal{H}(\overline{\mathbb{F}}_{q^2})$ lying over $P_{(a,b)}$, the following proposition describes the local power series expansion of the functions x_a and f_0 at $Q_{(A,B)}$, with respect to the local parameter $T := \frac{u-A}{A}$. In this proposition as well as in the remainder of this article, whenever we write $f = h + O(T^n)$, we mean that $v_{P_{(a,b)}}(f - h) \geq n$.

Proposition 2.12. *Let $P_{(a,b)} \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \setminus \mathcal{O}$ and $Q_{(A,B)}$ a point of $\mathcal{H}$ lying over $P_{(a,b)}$. Consider the functions x_a, f_0 and $T := \frac{u-A}{A}$, which is a local parameter at $Q_{(A,B)}$. Then, the local power series expansions of x_a and f_0 at $Q_{(A,B)}$ with respect to T are*

$$\begin{aligned} x_a &= 3T + 3T^2 + T^3, \\ f_0 &= 3T^2 + (\alpha(P_{(a,b)}) + 1)T^3 + O(T^q), \end{aligned} \tag{2.13}$$

where $\alpha(P_{(a,b)})$ is as defined in equation (2.10).

Proof. For convenience, we will simply write α instead of $\alpha(P_{(a,b)})$ in this proof. We start by computing the local power series expansions of the functions $x - a$ and $y - b$ with respect to the local parameter $T := (u - A)/A$ at $Q_{(A,B)}$. We have:

$$\begin{aligned} x_a = \frac{x-a}{a} = \frac{x-A^3}{A^3} = \frac{u^3-A^3}{A^3} &= \frac{(u-A)^3 + 3A(u-A)^2 + 3A^2(u-A)}{A^3} \\ = 3T + 3T^2 + T^3 \end{aligned}$$

and

$$\begin{aligned} y - b = uv - AB &= (u-A)(v-B) + B(u-A) + A(v-B) - AB + AB \\ &= A(v-B)(T+1) + ABT. \end{aligned} \tag{2.14}$$

Moreover, from $v^{q+1} + u^{q+1} + 1 = 0$, we obtain

$$(u-A)^{q+1} - A^{q+1} + A^q u + A u^q + (v-B)^{q+1} - B^{q+1} + B^q v + B v^q + 1 = 0$$

or equivalently

$$A^{q+1}T^{q+1} + (v-B)^{q+1} + A^{q+1}T^q + B(v-B)^q + A^{q+1}T + B^q(v-B) = 0$$

which gives $v - B = -\frac{A^{q+1}}{B^q}T + O(T^q)$. Combining this with equation (2.14), we obtain

$$\begin{aligned} y - b = A(v-B)(T+1) + ABT &= -A\frac{A^{q+1}}{B^q}T(T+1) + ABT + O(T^q) \\ &= A\left(B - \frac{A^{q+1}}{B^q}\right)T - \frac{A^{q+2}}{B^q}T^2 + O(T^q). \end{aligned}$$

We can now compute also the local power series expansion of the function f_0 at $Q_{(A,B)}$ with respect to the local parameter T. Using equation (2.11) and the previously computed expansions of x_a and $y - b$, we find

$$\begin{aligned} f_0 &= (1-\alpha)(3\left(A^{q+1}+1\right)T^2 + \left(2A^{q+1}+1\right)T^3) + O(T^q) \\ &= 3T^2 + (\alpha+1)T^3 + O(T^q), \end{aligned}$$

where in the final equality we used that $\alpha = A^{q+1}/(1 + A^{q+1})$. □

In the following proposition, we compute the divisors of several functions that we will use later. We will use the divisor D_∞ defined in equation (2.7).

Proposition 2.15. *In the above notations, the principal divisors of the functions x, x_a, y, $y - b$ and f_0 in $\mathbb{F}_{q^2}(\mathcal{X}_3)$ are:*

$$(x_a) = \begin{cases} P_{(a,b)} + \sum_{\xi^{q+1}=1,\ \xi \neq 1} P_{(a,\xi b)} - 3D_\infty \quad \text{if} \quad a^m \neq -1, \\ \\ (q+1)P_{(a,0)} - 3D_\infty \quad \text{if} \quad a^m = -1, \end{cases} \tag{2.16}$$

and

$$\begin{aligned} (x) &= 3\sum_{i=j}^{m} P_0^j - 3D_\infty, \\ (y) &= \sum_{j=1}^{m} P_0^j + \sum_{a^m+1=0} P_{(a,0)} - 2D_\infty, \\ (y-b) &= P_{(a,b)} + \tilde{E}_b - 2D_\infty, \end{aligned} \tag{2.17}$$

where $\tilde{E}_b \in \mathrm{Div}(\mathcal{X}_3)$ is an effective divisor of degree $2m - 1$. Moreover, if $P_{(a,b)} \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \backslash \mathcal{O}$ and $\alpha(P_{(a,b)}) \neq -1$, then $P_{(a,b)} \notin \mathrm{supp}(\tilde{E}_b)$. Further, for $P_{(a,b)} \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \backslash \mathcal{O}$, let f_0 be the function defined in equation (2.11). Then

$$(f_0) = 2P_{(a,b)} + E_0 - 3D_\infty, \tag{2.18}$$

where $E_0 \in \mathrm{Div}(\mathcal{X}_3)$ is an effective divisor such that $P_{(a,b)} \notin \mathrm{supp}(E_0)$.

Proof. To find the divisors of x_a and x, observe that $\mathbb{F}_{q^2}(\mathcal{X}_3)/\mathbb{F}_{q^2}(x)$ is a Kummer extension of degree $q+1$. Then, it is sufficient to note that the zeros of $x^m + 1$ are totally ramified in this extension, while, the zero and the pole of x have ramification index 3. No further ramification occurs as $y^{q+1} = -x^m(x^m + 1)$. This equation also gives the divisor of y. It is not clear that the divisor of $y-b$ is of the form as stated in the proposition, but it might happen that $P_{(a,b)} \in \mathrm{supp}(\tilde{E}_b)$. In this case, the polynomial $f(x) := x^{2m}+x^m+b^{q+1}$ would have a as a multiple root. Since $3f'(x) = x^{m-1}(2x^m + 1)$ and $P_{(a,b)} \notin \mathcal{O}$, this can only happen if $2a^m + 1 = 0$. Using that $\alpha(P_{(a,b)}) + 1 = (2a^m + 1)/(a^m + 1)$, the result on the divisor of $y - b$ follows.

Finally, from equation (2.13), we know that $v_{P_{(a,b)}}(f_0) = 2$ and, as f_0 is a linear combination of x_a and $y - b$, by the triangle inequality we also know that $v_{P_\infty^j}(f_0) = -3$ and that f_0 has no poles outside the P_∞^j, $1 \leq j \leq m$. Hence, equation (2.18) follows. □

Corollary 2.19. *Let $\mathcal{O}$ be the set defined in equation (2.5). Then $|\mathcal{O}| = q+1$ and $\mathcal{O}$ is an orbit of the automorphism group G defined in Lemma 2.6, in its natural action on the points of $\mathcal{X}_3$.*

Proof. We observe that the Galois group of the extension $\mathbb{F}_{q^2}(\mathcal{X}_3)/\mathbb{F}_{q^2}(x)$, that is the cyclic group generated by $(x, y) \longmapsto (x, \delta y)$, where δ is a primitive $(q+1)$-th root of unity, fixes the set $\mathcal{O}_m$ point-wise, while it acts transitively on the sets $\mathcal{O}_0$ and $\mathcal{O}_\infty$. The group A as defined in Lemma 2.6, acts transitively on the set $\mathcal{O}_m$ because it maps x to γx, where $\gamma^m = 1$. The automorphism θ_2 maps x to $1/x$ and hence from equation (2.17) merges the two orbits $\mathcal{O}_0$ and $\mathcal{O}_\infty$ under the action of G. The automorphism θ_3 instead acts as a cycle of order 3 on $\mathcal{O}_0$, $\mathcal{O}_\infty$ and $\mathcal{O}_m$. This can be seen from equation (2.17) and the fact that θ_3 maps x to y^3/x^2. As a result, all the three considered sets are merged into one orbit under the action of G. □

Remark 2.20. Let $\bar{a} \in \mathbb{F}_{q^2}$ be such that $\bar{a}^m = -1$. Then, the Fundamental Equation [15, Page xvii (ii)] ensures that, for any point $P_{(a,b)} \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \setminus \mathcal{X}_3(\mathbb{F}_{q^2})$, there exists a function $\phi_{P_{(a,b)}} \in \mathbb{F}_{q^2}(\mathcal{X}_3)$ such that

$$(\phi_{P_{(a,b)}}) = qP_{(a,b)} + \Phi(P_{(a,b)}) - (q+1)P_{(\bar{a},0)}.$$

Hence, we can consider the following function in $\mathbb{F}_{q^2}(\mathcal{X}_3)$, that will be useful later:

$$F_{P_{(a,b)}} := \phi_{P_{(a,b)}} \cdot x_{\bar{a}}. \tag{2.21}$$

By Proposition 2.15, the principal divisor of $F_{P_{(a,b)}}$ is

$$(F_{P_{(a,b)}}) = qP_{(a,b)} + \Phi(P_{(a,b)}) - 3\sum_{j=1}^{m} P_\infty^j.$$

2.2. Regular differentials and gaps

In this subsection, we recall a fundamental result relating regular differentials on a curve and the gaps at a point of the curve. More specifically, in Lemma 2.23 we compute a particular canonical divisor on $\mathcal{X}_3$ and, in Corollary 2.24, we show how to use this for determining gaps at certain points of the curve. In particular, Corollary 2.24 will be crucial for the results in Section 5.

Proposition 2.22. *[27, Corollary 14.2.5] Let $\mathcal{X}$ be an algebraic curve of genus $g(\mathcal{X})$ defined over a field $\mathbb{K}$. Let P be a point of $\mathcal{X}$ and w be a regular differential on $\mathcal{X}$. Then $v_P(w)+1$ is a gap at P.*

Lemma 2.23. *The divisor $(q-2)D_\infty$ is canonical. More precisely*

$$\left(\frac{ydx}{x(x^m+1)}\right) = (q-2)D_\infty.$$

Proof. The result follows directly from the fact that $\mathbb{F}_{q^2}(\mathcal{X}_3)/\mathbb{F}_{q^2}(x)$ is a Kummer extension of degree $q+1$. Indeed, as observed in the proof of Proposition 2.15, we have that the zeros of x^m+1 in $\mathbb{F}_{q^2}(x)$ are totally ramified in the extension, the zeros and the poles of x have ramification exponent 3 and the points that are not zeros of $x^m(x^m+1)$ split completely. Hence, we have

$$(dx) = 2\sum_{j=1}^{m} P_0^j + q\sum_{a^m+1=0} P_{(a,0)} - 4D_\infty$$

and the claim now follows from direct computation using Proposition 2.15. □

Corollary 2.24. *Let P be a point of $\mathcal{X}_3$ not in $\mathcal{O}_\infty$. Then for any $h \in L((q-2)D_\infty)$, the integer $v_P(h)+1$ is a gap of Weierstrass semigroup at P.*

Proof. From Proposition 2.22 and Lemma 2.23 it is enough to consider the regular differential

$$w := \frac{hydx}{x(x^m+1)}.$$

Since $v_P(w) = v_P(h)$, the corollary follows. □

3. Two families of functions in $\mathbb{F}_{q^2}(\mathcal{X}_3)$

The aim of this section is to prove Theorem 3.12 and Theorem 3.19, that introduce two families of functions in $\mathbb{F}_{q^2}(\mathcal{X}_3)$ with prescribed vanishing orders in certain points of the curve. These functions will be crucial for the computation of the Weierstrass semigroups at the points of $\mathcal{X}_3 \setminus \mathcal{O}$.

We start by giving the following definition, introducing some functions that will be practical to use in the proofs of Theorem 3.12 and Theorem 3.19.

Definition 3.1. Let $i \in \mathbb{Z}$. Further, let $\mathbb{F}$ be a field of characteristic different from three and assume that it contains a primitive cube root of unity, which we will denote by ζ_3. Then we define the following rational functions in $\mathbb{F}(s)$:

$$\mathcal{P}_i(s) := \frac{(s+\zeta_3)^{3i} - (s+\zeta_3^2)^{3i}}{3(\zeta_3-\zeta_3^2)s(s-1)}$$

and

$$\mathcal{Q}_i(s) := \frac{\left(\frac{1-\zeta_3}{3}\right)(s+\zeta_3)^{3i-1} + \left(\frac{1-\zeta_3^2}{3}\right)(s+\zeta_3^2)^{3i-1}}{s-1}.$$

Note that it strictly speaking is not necessary to assume that the field $\mathbb{F}$ contains a primitive cube root of unity. If it does not, the above definition makes sense over the larger field $\mathbb{F}(\zeta_3)$, but actually elementary Galois theory can be used to show $\mathcal{P}_i(s)$ and $\mathcal{Q}_i(s)$ are in $\mathbb{F}(s)$.

Example 3.2. Assume $\mathbb{F} = \mathbb{Q}$. Then $\mathcal{P}_0(s) = 0$, $\mathcal{P}_1(s) = 1$, $\mathcal{P}_2(s) = 2s^3 - 3s^2 - 3s + 2$ and $\mathcal{P}_3(s) = 3s^6 - 9s^5 - 9s^4 + 33s^3 - 9s^2 - 9s + 3$. Moreover, $\mathcal{Q}_1(s) = s + 1$, $\mathcal{Q}_2(s) = s^4 + s^3 - 9s^2 + s + 1$, $\mathcal{Q}_3(s) = s^7 + s^6 - 27s^5 + 29s^4 + 29s^3 - 27s^2 + s + 1$, and $\mathcal{Q}_0(s) = (s^2 - s + 1)^{-1}$.

In fact, as illustrated in this example, for positive values of i the rational functions $\mathcal{P}_i(s)$ and $\mathcal{Q}_j(s)$ are polynomials in s. We investigate this further in the following lemma.

Lemma 3.3. *Let $i \in \mathbb{Z}_{>0}$. Then $\mathcal{P}_i(s)$ is a nonzero polynomial of degree at most $3i - 3$, while $\mathcal{Q}_i(s)$ is a nonzero polynomial of degree $3i - 2$.*

Proof. It is easy to see that for any $i \in \mathbb{Z}_{>0}$, the polynomial $\tilde{\mathcal{P}}_i(s) := (s+\zeta_3)^{3i} - (s+\zeta_3^2)^{3i}$ has at most degree $3i - 1$. It is not the zero polynomial, since if s is substituted by $-\zeta_3$, one obtains

$$\tilde{\mathcal{P}}_i(-\zeta_3) = 0^{3i} - (-\zeta_3 + \zeta_3^2)^{3i} = -(-1 + \zeta_3)^{3i}, \tag{3.4}$$

which is not zero, as $\zeta_3 \neq 1$. Here we used that the field $\mathbb{F}$ does not have characteristic three. It is easy to see that $\tilde{\mathcal{P}}_i(0) = 0$, while

$$\tilde{\mathcal{P}}_i(1) = (1 + \zeta_3)^{3i} - (1 + \zeta_3^2)^{3i} = (-\zeta_3^2)^{3i} - (-\zeta_3)^{3i} = (-1)^i - (-1)^i = 0.$$

We may conclude that $\mathcal{P}_i(s)$ is a polynomial of degree at most $3i - 3$. Similarly, the polynomial $\tilde{\mathcal{Q}}_i(s) := \frac{1-\zeta_3}{3}(s + \zeta_3)^{3i-1} + \frac{1-\zeta_3^2}{3}(s + \zeta_3^2)^{3i-1}$ is a polynomial of degree $3i - 1$ having 1 as a root. Hence $\mathcal{Q}_i(s)$ is a polynomial of degree $3i - 2$. □

It is not hard to see that the coefficient of s^{3i-3} of the polynomial $\mathcal{P}_i(s)$ equals $3i(\zeta_3 - \zeta_3^2)$. Hence if the characteristic of the field $\mathbb{F}$, which already is assumed to be distinct from three, is zero or does not divide i, then the degree of $\mathcal{P}_i(s)$ is exactly $3i - 3$. Since we will work over the finite field $\mathbb{F}_{q^2}$, where $q \equiv 2 \pmod 3$, it may well happen that $\deg \mathcal{P}_i(s) < 3i - 3$.

The following lemma gives a relation between the rational functions just introduced that will come in handy later.

Lemma 3.5. *Let $i, j, \ell \in \mathbb{Z}$. Then*

$$\mathcal{P}_i(s)\mathcal{P}_{\ell+j}(s) - \mathcal{P}_j(s)\mathcal{P}_{\ell+i}(s) = (s^2 - s + 1)^{3j}\mathcal{P}_{i-j}(s)\mathcal{P}_\ell(s) \tag{3.6}$$

and

$$\mathcal{P}_i(s)\mathcal{Q}_{\ell+j}(s) - \mathcal{P}_j(s)\mathcal{Q}_{\ell+i}(s) = (s^2-s+1)^{3j}\mathcal{P}_{i-j}(s)\mathcal{Q}_\ell(s). \tag{3.7}$$

Proof. For convenience, we will simply write $\mathcal{P}_i$ and $\mathcal{Q}_j$ instead of $\mathcal{P}_i(s)$ and $\mathcal{Q}_i(s)$ in this proof. We prove the second identity only, since the first identity can be proven in a very similar way with simpler looking intermediate expressions. First of all, using Definition 3.1 and writing $S_1 = s+\zeta_3$, $S_2 = s+\zeta_3^2$, one obtains by direct computation

$$3(\zeta_3-\zeta_3^2)s(s-1)^2\mathcal{P}_i\mathcal{Q}_{\ell+j} = \\ \frac{1-\zeta_3}{3}S_1^{3i+3j+3\ell-1} + \frac{1-\zeta_3^2}{3}S_1^{3i}S_2^{3j+3\ell-1} - \frac{1-\zeta_3}{3}S_2^{3i}S_1^{3j+3\ell-1} - \frac{1-\zeta_3^2}{3}S_2^{3i+3j+3\ell-1}$$

and

$$3(\zeta_3-\zeta_3^2)s(s-1)^2\mathcal{P}_j\mathcal{Q}_{\ell+i} = \\ \frac{1-\zeta_3}{3}S_1^{3i+3j+3\ell-1} + \frac{1-\zeta_3^2}{3}S_1^{3j}S_2^{3i+3\ell-1} - \frac{1-\zeta_3}{3}S_2^{3j}S_1^{3i+3\ell-1} - \frac{1-\zeta_3^2}{3}S_2^{3i+3j+3\ell-1}.$$

Hence

$$\begin{aligned} &3(\zeta_3-\zeta_3^2)s(s-1)^2(\mathcal{P}_i\mathcal{Q}_{\ell+j} - \mathcal{P}_j\mathcal{Q}_{\ell+i}) = \\ &(S_1S_2)^{3j}\left(\frac{1-\zeta_3}{3}(S_1^{3\ell+3i-3j-1} - S_2^{3i-3j}S_1^{3\ell-1}) + \frac{1-\zeta_3^2}{3}(S_1^{3i-3j}S_2^{3\ell-1} - S_2^{3\ell+3i-3j-1})\right) \\ &\qquad = (S_1S_2)^{3j}(S_1^{3(i-j)} - S_2^{3(i-j)})\left(\frac{1-\zeta_3}{3}S_1^{3\ell-1} + \frac{1-\zeta_3^2}{3}S_2^{3\ell-1}\right) \\ &\qquad = 3(\zeta_3-\zeta_3^2)s(s-1)^2(s^2-s+1)^{3j}\mathcal{P}_{i-j}\mathcal{Q}_\ell. \end{aligned}$$

For the last equality, note that $S_1S_2 = s^2-s+1$. □

Remark 3.8. For any $i \in \mathbb{Z}_{>0}$, the polynomials $\mathcal{P}_i(s)$ and $\mathcal{Q}_i(s)$ have no common roots. Indeed, this is clear for $i=1$, since $\mathcal{P}_1(s)=1$. If $i \geq 2$, Lemma 3.5 applied with $\ell = 0$ and $j = i-1$, implies that $\mathcal{P}_i(s)\mathcal{Q}_{i-1}(s) - \mathcal{P}_{i-1}(s)\mathcal{Q}_i(s) = (s^2-s+1)^{3i-4}$. Here we used that $\mathcal{Q}_0(s) = (s^2-s+1)^{-1}$. Hence the only possible common roots of $\mathcal{P}_i(s)$ and $\mathcal{Q}_i(s)$ could be $-\zeta_3$ or $-\zeta_3^2$, the roots of s^2-s+1. However, equation (3.4) implies that $\mathcal{P}_i(-\zeta_3) \neq 0$ and similarly one sees that $\mathcal{P}_i(-\zeta_3^2) \neq 0$.

Remark 3.9. Let $\mathbb{F} = \overline{\mathbb{F}}_{q^2}$ be the algebraic closure of $\mathbb{F}_{q^2}$. Then for any $\alpha \in \mathbb{F} \setminus \{0, 1, -\zeta_3, -\zeta_3^2\}$, there exists $i > 0$ such that $\mathcal{P}_{i+1}(\alpha) = 0$. Indeed, for such α one has $\mathcal{P}_{i+1}(\alpha) = 0$ if and only if $((\alpha+\zeta_3)/(\alpha+\zeta_3^2))^{3i+3} = 1$. Since any nonzero element of $\mathbb{F}$ has a finite multiplicative order, the existence of i follows. Moreover, since $\mathcal{P}_1(s) = 1$, we see that $i > 0$.

This remark motivates the following definition:

Definition 3.10. Let $\alpha \in \overline{\mathbb{F}}_{q^2} \setminus \{0, 1, -\zeta_3, -\zeta_3^2\}$. Then we define the $\mathcal{P}$-order of α as the smallest positive integer i such that $\mathcal{P}_{i+1}(\alpha) = 0$.

Later we will apply the notion of a $\mathcal{P}$-order in case $\alpha = \alpha(P_{(a,b)})$. The following lemma is a first source of information in this setting.

Lemma 3.11. *Let i be a positive integer. The number of $P_{(a,b)} \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \setminus \mathcal{O}$ such that $\alpha(P_{(a,b)})$ has $\mathcal{P}$-order i is equal to $(q+1)^2\varphi(i+1)$ if $\gcd(i+1,p) = 1$ and 0 otherwise. Here $\varphi(\cdot)$ denotes Euler's totient function. Moreover, $P_{(a,b)} \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \setminus \mathcal{O}$ is $\mathbb{F}_{q^2}$-rational if and only if $\alpha(P_{(a,b)})^2 - \alpha(P_{(a,b)}) + 1 = 0$ or its $\mathcal{P}$-order i satisfies that $i+1$ divides m.*

Proof. If $\alpha := \alpha(P_{(a,b)})$ has $\mathcal{P}$-order i for some positive integer i, then $\alpha \notin \{0, 1, -\zeta_3, -\zeta_3^2\}$ and $P_{(a,b)} \notin \mathcal{O}$. As observed in Remark 3.9, we have $\mathcal{P}_{i+1}(\alpha) = 0$ if and only if $((\alpha+\zeta_3)/(\alpha+\zeta_3^2))^{3i+3} = 1$. If the characteristic p divides $i+1$, we see that $((\alpha+\zeta_3)/(\alpha+\zeta_3^2))^{3(i+1)/p} = 1$, implying that $\mathcal{P}_j(\alpha) = 0$ for some j strictly smaller than $i+1$. By definition of $\mathcal{P}$-order, this is impossible. If $\gcd(p, i+1) = 1$, the α that have $\mathcal{P}$-order i are precisely those satisfying that $((\alpha+\zeta_3)/(\alpha+\zeta_3^2))^3$ is a primitive $(i+1)$-th root of unity. Hence there are $3\varphi(i+1)$ many α with $\mathcal{P}$-order i. Since $\alpha = a^m/(1+a^m)$ and $\alpha \notin \{0, 1\}$, for each such α, there are m distinct possibilities for a. Since $P_{(a,b)} \notin \mathcal{O}$, for each such a, there are $q+1$ distinct possibilities for b. This proves the first part of the lemma.

Now suppose that $P_{(a,b)} \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \setminus \mathcal{O}$ is $\mathbb{F}_{q^2}$-rational and $\alpha^2 - \alpha + 1 \neq 0$. First of all, we claim that in this case $\alpha \in \mathbb{F}_q$. Indeed, since $a, b \in \mathbb{F}_{q^2}$, we obtain that $a^{3m} = a^{q+1} \in \mathbb{F}_q$ and $a^{2m} + a^m = -b^{q+1} \in \mathbb{F}_q$. But then $a^m = (a^{3m} + a^{2m} + a^m)/(a^{2m} + a^m + 1) \in \mathbb{F}_q$. Here we used that $a^{2m} + a^m + 1 \neq 0$, which follows from the assumption that $\alpha^2 - \alpha + 1 \neq 0$. Now $a^m \in \mathbb{F}_q$, implies $\alpha = a^m/(1+a^m) \in \mathbb{F}_q$. In particular $\alpha^q = \alpha$. This implies that

$$\left(\frac{\alpha+\zeta_3}{\alpha+\zeta_3^2}\right)^q = \frac{\alpha^q + \zeta_3^q}{\alpha^q + \zeta_3^{2q}} = \frac{\alpha+\zeta_3^2}{\alpha+\zeta_3},$$

which is exactly the inverse of $\frac{\alpha+\zeta_3}{\alpha+\zeta_3^2}$. Hence $\left(\frac{\alpha+\zeta_3}{\alpha+\zeta_3^2}\right)^{3m} = \left(\frac{\alpha+\zeta_3}{\alpha+\zeta_3^2}\right)^{q+1} = 1$. This shows that $i+1$ divides m.

Conversely, if $\alpha^2 - \alpha + 1 = 0$, then $P_{(a,b)} \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \setminus \mathcal{O}$ satisfies $a^{2m} + a^m + 1 = 0$, which in turn implies $b^{q+1} = 1$. Hence $a, b \in \mathbb{F}_{q^2}$. If $\alpha^2 - \alpha + 1 \neq 0$ and $i+1$ divides m, then $3(i+1)$ divides $q+1$ and $\left(\frac{\alpha+\zeta_3}{\alpha+\zeta_3^2}\right)^{3(i+1)} = 1$. Hence $\left(\frac{\alpha+\zeta_3}{\alpha+\zeta_3^2}\right)^{q+1} = 1$, which after clearing denominators amounts to the equation $(\alpha+\zeta_3)^{q+1} - (\alpha+\zeta_3^2)^{q+1} = 0$. This is a polynomial in α of degree q and we have already seen that this equation is satisfied for all $\alpha \in \mathbb{F}_q$. We may conclude that $\alpha \in \mathbb{F}_q$. But then $a^m \in \mathbb{F}_q$, which implies that $b^{q+1} = -a^{2m} - a^m \in \mathbb{F}_q$. We conclude that also in this case $P_{(a,b)}$ is an $\mathbb{F}_{q^2}$-rational point of $\mathcal{X}_3$. □

Next, we use the polynomials $\mathcal{P}_j(s)$ and $\mathcal{Q}_j(s)$ to investigate the existence of functions that will be useful later when determining gaps at points $P_{(a,b)} \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \setminus \mathcal{O}$.

Theorem 3.12. *Let $P_{(a,b)} \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \setminus \mathcal{O}$ and suppose that $\alpha(P_{(a,b)})^2 - \alpha(P_{(a,b)}) + 1 \neq 0$. Further, let i be the $\mathcal{P}$-order of $\alpha(P_{(a,b)})$. If $i \leq m-2$, then there exists a function $f_i \in L((3i+3)D_\infty)$ such that $v_{P_{(a,b)}}(f_i) = 3i+3$. Moreover, for each $j \in \mathbb{Z}$ with $0 \leq j \leq \min\{i-1, m-2\}$, there exists a function $f_j \in L((3j+3)D_\infty)$ with $v_{P_{(a,b)}}(f_j) = 3j+2$.*

Proof. Throughout the proof we simplify the notation by writing α instead of $\alpha(P_{(a,b)})$. In a similar vein, we will write $\mathcal{P}_j$ and $\mathcal{Q}_j$, rather than $\mathcal{P}_j(\alpha)$ and $\mathcal{Q}_j(\alpha)$.

Let $Q_{(A,B)}$ be a point of $\mathcal{H}$ lying over $P_{(a,b)}$ and let $T := \frac{u-A}{A}$, which is a local parameter at $Q_{(A,B)}$. For each j such that $0 \leq j \leq i$, we claim that there exists a function $f_j \in L((3j+3)D_\infty)$ such that the local power series expansion of f_j at $Q_{(A,B)}$ with respect to the local parameter T is

$$f_j = 3\mathcal{P}_{j+1}T^{3j+2} + \mathcal{Q}_{j+1}T^{3j+3} + O(T^q). \tag{3.13}$$

Note that by definition of the $\mathcal{P}$-order, this will imply that

$$f_i = \mathcal{Q}_{i+1}T^{3i+3} + O(T^q). \tag{3.14}$$

This is sufficient to prove the theorem since, as observed in Remark 2.4, $v_{Q_{(A,B)}}(f_j) = v_{P_{(a,b)}}(f_j)$ and $3j+3 < q$ for all j under consideration.

First of all, note that, for $j = 0$, we can take f_0 to be exactly the function defined in equation (2.11) and whose local power series expansion with respect to T was computed in equation (2.13). To show the result for $j = 1$, we define

$$f_1 := -9x_a^2 + 27f_0 - 3(\alpha-5)x_a f_0 + (\alpha^2-\alpha-5)f_0^2.$$

Elementary calculations show that the local power series expansion of f_1 at $Q_{(A,B)}$ with respect to T is precisely

$$f_1 = 3\mathcal{P}_2T^5 + \mathcal{Q}_2T^6 + O(T^q).$$

For $j = 2$, we define

$$f_2 := (\alpha+1)^{-3}\left(-27\mathcal{P}_2f_1 + 3\mathcal{P}_2^2f_0^2x_a - 3\mathcal{P}_2(\alpha^4+\alpha^3-4\alpha^2-4\alpha+3)f_0^3\right) \\ + (7\alpha^2-16\alpha+7)f_1f_0.$$

A somewhat lengthy, but elementary, calculation shows that the local power series expansion of f_2 equals

$$f_2 = 3\mathcal{P}_3T^8 + \mathcal{Q}_3T^9 + O(T^q).$$

For $3 \leq j \leq i$, we assume now that f_{j-1} and f_{j-2} have the form claimed in equation (3.13) and we construct inductively the remaining functions f_j in the following way, defining:

$$f_j := -\frac{\mathcal{P}_j f_{j-2} f_1 - \mathcal{P}_2 \mathcal{P}_{j-1} f_{j-1} f_0}{(\alpha^2 - \alpha + 1)^2 \mathcal{P}_{j-2}}.$$

The idea of choosing the functions $f_{j-2}f_1$ and $f_{j-1}f_0$ is that the vanishing order at $Q_{(A,B)}$ is $3j+1$ for both. Hence, a suitable linear combination of them will vanish with order at least $3j+2$. Moreover, as $f_{j-2}f_1$ and $f_{j-1}f_0$ lie in $L((3j+3)D_\infty)$, a linear combination of them does as well. Therefore, we only need to show that

$$\mathcal{P}_j f_{j-2} f_1 - \mathcal{P}_2 \mathcal{P}_{j-1} f_{j-1} f_0 = -(\alpha^2 - \alpha + 1)^2 \mathcal{P}_{j-2} \left(3\mathcal{P}_{j+1} T^{3j+2} + \mathcal{Q}_{j+1} T^{3j+3} + O(T^q)\right).$$

The local power series expansion of $\mathcal{P}_j f_{j-2} f_1 - \mathcal{P}_2 \mathcal{P}_{j-1} f_{j-1} f_0$ with respect to T can be obtained from the expansions of the functions $f_{j-2}f_1$ and $f_{j-1}f_0$, which are:

$$\begin{aligned} f_{j-2}f_1 &= \left(3\mathcal{P}_{j-1}T^{3j-4} + \mathcal{Q}_{j-1}T^{3j-3} + O(T^q)\right)\left(3\mathcal{P}_2 T^5 + \mathcal{Q}_2 T^6 + O(T^q)\right) \\ &= 9\mathcal{P}_2\mathcal{P}_{j-1}T^{3j+1} + (3\mathcal{P}_{j-1}\mathcal{Q}_2 + 3\mathcal{P}_2\mathcal{Q}_{j-1})T^{3j+2} + \mathcal{Q}_2\mathcal{Q}_{j-1}T^{3j+3} + O(T^q), \\ f_{j-1}f_0 &= \left(3\mathcal{P}_j T^{3j-1} + \mathcal{Q}_j T^{3j} + O(T^q)\right)\left(3T^2 + \mathcal{Q}_1 T^3 + O(T^q)\right) \\ &= 9\mathcal{P}_j T^{3j+1} + (3\mathcal{P}_j\mathcal{Q}_1 + 3\mathcal{Q}_j)T^{3j+2} + \mathcal{Q}_1\mathcal{Q}_j T^{3j+3} + O(T^q). \end{aligned}$$

Hence, we have

$$\begin{aligned} \mathcal{P}_j f_{j-2} f_1 - \mathcal{P}_2 \mathcal{P}_{j-1} f_{j-1} f_0 = {} & 3(\mathcal{P}_{j-1}\mathcal{P}_j\mathcal{Q}_2 + \mathcal{P}_2\mathcal{P}_j\mathcal{Q}_{j-1} - \mathcal{P}_2\mathcal{P}_{j-1}\mathcal{P}_j\mathcal{Q}_1 - \mathcal{P}_2\mathcal{P}_{j-1}\mathcal{Q}_j)T^{3j+2} \\ & + \left(\mathcal{P}_j\mathcal{Q}_{j-1}\mathcal{Q}_2 - \mathcal{P}_{j-1}\mathcal{P}_2\mathcal{Q}_j\mathcal{Q}_1\right)T^{3j+3} + O(T^q). \end{aligned}$$

We are therefore left to prove the two following identities:

$$3\left(\mathcal{P}_{j-1}\mathcal{P}_j\mathcal{Q}_2 + \mathcal{P}_2\mathcal{P}_j\mathcal{Q}_{j-1} - \mathcal{P}_2\mathcal{P}_{j-1}\mathcal{P}_j\mathcal{Q}_1 - \mathcal{P}_2\mathcal{P}_{j-1}\mathcal{Q}_j\right) = -3(\alpha^2 - \alpha + 1)^2\mathcal{P}_{j-2}\mathcal{P}_{j+1} \tag{3.15}$$

and

$$\mathcal{P}_j\mathcal{Q}_{j-1}\mathcal{Q}_2 - \mathcal{P}_{j-1}\mathcal{P}_2\mathcal{Q}_j\mathcal{Q}_1 = -(\alpha^2 - \alpha + 1)^2\mathcal{P}_{j-2}\mathcal{Q}_{j+1}. \tag{3.16}$$

This can be conveniently done by using Lemma 3.5. Indeed, consider first equation (3.15) and use identity (3.7) as

$$\mathcal{P}_j\mathcal{Q}_2 - \mathcal{P}_2\mathcal{Q}_j = \mathcal{P}_{j-2}\mathcal{Q}_0 \cdot (s^2 - s + 1)^6,$$

i.e., with indices $(j, 2, 0)$ (listed in order as in the statement of Lemma 3.5). Then, we obtain

$$\begin{aligned}\mathcal{P}_{j-1}\mathcal{P}_j\mathcal{Q}_2 - \mathcal{P}_2\mathcal{P}_{j-1}\mathcal{Q}_j &= \mathcal{P}_{j-1}(\mathcal{P}_j\mathcal{Q}_2 - \mathcal{P}_2\mathcal{Q}_j)\\ &= \mathcal{P}_{j-1}\cdot(\alpha^2-\alpha+1)^5\mathcal{P}_{j-2}.\end{aligned} \tag{3.17}$$

By using again equation (3.7), this time with indices $(j-1,1,0)$, we can also rewrite

$$\begin{aligned}\mathcal{P}_2\mathcal{P}_j\mathcal{Q}_{j-1} - \mathcal{P}_2\mathcal{P}_{j-1}\mathcal{P}_j\mathcal{Q}_1 &= \mathcal{P}_2\mathcal{P}_j\mathcal{Q}_{j-1}\mathcal{P}_1 - \mathcal{P}_2\mathcal{P}_{j-1}\mathcal{P}_j\mathcal{Q}_1\\ &= -\mathcal{P}_2\mathcal{P}_j(\mathcal{P}_{j-1}\mathcal{Q}_1 - \mathcal{P}_1\mathcal{Q}_{j-1})\\ &= -\mathcal{P}_2\mathcal{P}_j\cdot(\alpha^2-\alpha+1)^2\mathcal{P}_{j-2}.\end{aligned} \tag{3.18}$$

Then, by equations (3.17) and (3.18), we have that equation (3.15) is equivalent to

$$\mathcal{P}_{j-1}\cdot(\alpha^2-\alpha+1)^5\mathcal{P}_{j-2} - \mathcal{P}_2\mathcal{P}_j\cdot(\alpha^2-\alpha+1)^2\mathcal{P}_{j-2} = -(\alpha^2-\alpha+1)^2\mathcal{P}_{j-2}\mathcal{P}_{j+1}.$$

Dividing out the factor $(\alpha^2-\alpha+1)^2\mathcal{P}_{j-2}$ both in the right hand side and the left hand side of this equality and rearranging the terms, we obtain

$$\mathcal{P}_{j-1}\cdot(\alpha^2-\alpha+1)^3 = \mathcal{P}_2\mathcal{P}_j - \mathcal{P}_{j+1},$$

which holds by Lemma 3.5, as it is precisely identity (3.6) with indices $(j,1,1)$.

In order to prove equation (3.16), we can argue in a similar way. Indeed, we have:

$$\begin{aligned}\mathcal{P}_j\mathcal{Q}_{j-1}\mathcal{Q}_2 - \mathcal{P}_{j-1}\mathcal{P}_2\mathcal{Q}_j\mathcal{Q}_1 &= (\mathcal{P}_j\mathcal{Q}_2 - \mathcal{P}_2\mathcal{Q}_j + \mathcal{P}_2\mathcal{Q}_j)\mathcal{Q}_{j-1} - \mathcal{P}_{j-1}\mathcal{P}_2\mathcal{Q}_j\mathcal{Q}_1\\ &= \left(\mathcal{P}_{j-2}\cdot(\alpha^2-\alpha+1)^5 + \mathcal{P}_2\mathcal{Q}_j\right)\mathcal{Q}_{j-1} - \mathcal{P}_{j-1}\mathcal{P}_2\mathcal{Q}_j\mathcal{Q}_1,\end{aligned}$$

where the last equality follows from equation (3.7) with indices $(j,2,0)$. Moreover,

$$\begin{aligned}&\left(\mathcal{P}_{j-2}\cdot(\alpha^2-\alpha+1)^5 + \mathcal{P}_2\mathcal{Q}_j\right)\mathcal{Q}_{j-1} - \mathcal{P}_{j-1}\mathcal{P}_2\mathcal{Q}_j\mathcal{Q}_1 =\\ &\qquad \mathcal{P}_{j-2}\cdot(\alpha^2-\alpha+1)^5\mathcal{Q}_{j-1} - \mathcal{P}_2\mathcal{Q}_j\left(\mathcal{P}_{j-1}\mathcal{Q}_1 - \mathcal{P}_1\mathcal{Q}_{j-1}\right) =\\ &\qquad\qquad \mathcal{P}_{j-2}\cdot(\alpha^2-\alpha+1)^5\mathcal{Q}_{j-1} - \mathcal{P}_2\mathcal{Q}_j\mathcal{P}_{j-2}\cdot(\alpha^2-\alpha+1)^2,\end{aligned}$$

where the last equality follows from equation (3.7) with indices $(j-1,1,0)$. Finally, using again equation (3.7) with indices $(2,1,j-1)$, we have

$$\begin{aligned}&\mathcal{P}_{j-2}\cdot(\alpha^2-\alpha+1)^5\mathcal{Q}_{j-1} - \mathcal{P}_2\mathcal{Q}_j\mathcal{P}_{j-2}\cdot(\alpha^2-\alpha+1)^2 =\\ &-\mathcal{P}_{j-2}\cdot(\alpha^2-\alpha+1)^2\left(\mathcal{P}_2\mathcal{Q}_j - \mathcal{Q}_{j-1}\cdot(\alpha^2-\alpha+1)^3\mathcal{P}_1\right) = -\mathcal{P}_{j-2}\cdot(\alpha^2-\alpha+1)^2\mathcal{Q}_{j+1},\end{aligned}$$

which proves equation (3.16).

From this, equation (3.13) follows directly, while equation (3.14) follows observing that $\mathcal{P}_{i+1}=0$ by hypothesis and $\mathcal{Q}_{i+1}\neq 0$ by Remark 3.8. As we have already observed that, by construction, $f_j \in L((3j+3)D_\infty)$ for all j in $0 \le j \le i$, the proof of the theorem is then completed. □

The proof of the theorem does not work if $\alpha^2-\alpha+1=0$, but a very similar approach works as will become clear in the proof of the following result. Recall that, if $\alpha^2-\alpha+1=0$, then α is not a root of any $\mathcal{P}_i$, for all $i \in \mathbb{Z}_{>0}$.

Theorem 3.19. *Suppose that $P_{(a,b)}$ is a point on $\mathcal{X}_3$ such that $\alpha(P_{(a,b)})^2-\alpha(P_{(a,b)})+1=0$. Then, for every positive integer i such that $i \leq m-2$, there exists a function $g_i \in L((3i+3)D_\infty)$ with $v_{P_{(a,b)}}(g_i)=3i+2$.*

Proof. As before, in this proof we write α instead of $\alpha(P_{(a,b)})$ and $\mathcal{P}_j$, $\mathcal{Q}_j$ instead of $\mathcal{P}_j(\alpha)$, $\mathcal{Q}_j(\alpha)$. For each $i \in \mathbb{Z}_{\geq 0}$, we claim that there exists a function $g_i \in L((3i+3)D_\infty)$ such that the local power series expansion of g_i at $Q_{(A,B)}$ with respect to the local parameter T is:

$$g_i = 3T^{3i+2}+(\alpha+1)T^{3i+3}+O(T^q) \tag{3.20}$$

Denoting by f_0 and f_1, the functions constructed in the previous theorem, we see that $g_0=f_0$, while $g_1=(2\alpha-1)f_1/9$, since

$$(2\alpha-1)3\mathcal{P}_2 \equiv 27 \pmod{\alpha^2-\alpha+1}$$

and

$$(2\alpha-1)\mathcal{Q}_2 \equiv 9\alpha+9 \pmod{\alpha^2-\alpha+1}.$$

For $i \geq 2$, we assume now that g_{i-1} and g_{i-2} have the form claimed in equation (3.20) and we construct inductively the remaining functions g_i by taking a suitable linear combination of

$$g_{i-1}, \quad g_{i-2}\cdot g_0 \cdot x_a, \quad g_{i-2}\cdot g_0^2 \quad \text{and} \quad g_{i-1}\cdot g_0.$$

The point of choosing these four functions, is that their vanishing orders at $Q_{(A,B)}$ are $3i-1$, $3i-1$, $3i$ and $3i+1$ respectively. Therefore a suitable linear combination of them will vanish with order at least $3i+2$. Moreover, since the four function all lie in $L((3i+3)D_\infty)$, any linear combination of them does as well.

More in detail, if we set

$$g_i := (6\alpha-3)g_{i-1} - \frac{2\alpha-1}{3}g_{i-2}g_0x_a + \frac{3\alpha-2}{3}g_{i-2}g_0^2 - (\alpha-2)g_{i-1}g_0,$$

then a direct computation shows that equation (3.20) is satisfied. □

4. Weierstrass semigroups at the $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}_3$

In this section, we compute the Weierstrass semigroups at all the $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}_3$. We start with the determination of the semigroup at the points of the set $\mathcal{O}$ and then continue to all other $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}_3$. We will assume that q is at least five, so that $m \geq 2$. If $q = 2$, the curve $\mathcal{X}_3$ is an elliptic curve, so all Weierstrass semigroups are just $\{0\} \cup \mathbb{Z}_{\geq 2}$ in that case.

Remark 4.1. By the Fundamental Equation ([15, Page xvii (ii)]) and by [15, Proposition 10.9], it is well known that both q and $q+1$ are non-gaps at every $\mathbb{F}_{q^2}$-rational point of an $\mathbb{F}_{q^2}$-maximal curve. However, in Theorem 4.2 and in Lemma 4.3, we prove this fact again in the particular case of $\mathcal{X}_3$, as we show this with some easy explicit computations.

4.1. The Weierstrass semigroup at $P \in \mathcal{O}$

Theorem 4.2. *Let $P \in \mathcal{O}$. Then $H(P) = \langle q-2, q, q+1 \rangle$.*

Proof. We will prove that

$$H(P_{(a,0)}) = \langle q-2, q, q+1 \rangle$$

for $P_{(a,0)} \in \mathcal{O}$ a point such that $a^m + 1 = 0$, and hence the result will follow as, by Corollary 2.19, $\mathcal{O}$ is contained in an orbit of $\mathrm{Aut}(\mathcal{X}_3)$ and all the points in the same orbit have the same Weierstrass semigroup.

We start by showing that the semigroup $H := \langle q-2, q, q+1 \rangle$, that is to say, the semigroup generated by $q-2, q$ and $q+1$, is contained in $H(P_{(a,0)})$. Proposition 2.15 implies that the functions

$$\frac{1}{x-a}, \quad \frac{y}{x-a}, \quad \text{and} \quad \frac{y^3}{x(x-a)}$$

in $\mathbb{F}_{q^2}(\mathcal{X}_3)$ only have a pole at $P_{(a,0)}$ and of order $q+1$, q, and $q-2$ respectively. This shows that $q-2, q, q+1 \in H(P_{(a,0)})$, proving that $H \subseteq H(P_{(a,0)})$.

Hence to conclude the proof of the theorem it is sufficient to show that the number of gaps of semigroup H, also known as the genus of H, is equal to $g(\mathcal{X}_3)$. To do so, note that semigroup H is telescopic, since the sequence $(a_1, a_2, a_3) := (q-2, q+1, q)$ is a telescopic sequence. See for example [16, Section 5.4] for a short discussion on telescopic semigroups. Defining $d_0 = 0$, $d_1 = q-2$, $d_2 = \gcd(q-2, q+1) = 3$, and $d_3 = \gcd(q-2, q, q+1) = 1$, the genus of H is according to [16, Proposition 5.35] given by

$$g(H) = \frac{1}{2}\left(1 + \sum_{i=1}^{3} \left(\frac{d_{i-1}}{d_i} - 1\right) a_i\right) = g(\mathcal{X}_3). \quad \square$$

4.2. The Weierstrass semigroups at the points in $\mathcal{X}_3(\mathbb{F}_{q^2}) \setminus \mathcal{O}$

Lemma 4.3. *Let $P_{(a,b)} \in \mathcal{X}_3(\mathbb{F}_{q^2}) \setminus \mathcal{O}$. Then $q+1$ and q are contained in $H(P_{(a,b)})$.*

Proof. The fact that $q+1 \in H(P_{(a,b)})$ is simply a consequence of equation (2.8). To prove that $q \in H(P_{(a,b)})$, let $P_{(\bar{a},0)} \in \mathcal{X}_3(\mathbb{F}_{q^2})$ such that $\bar{a}^m + 1 = 0$ and consider the function

$$h_q := \frac{(x-a) f_{P_{(\bar{a},0)},1}}{f_{P_{(a,b)},1}(x-\bar{a})},$$

where the functions $f_{P_{(a,b)},1}$ and $f_{P_{(\bar{a},0)},1}$ are defined as in equation (2.8). Then, from equations (2.8), (2.16), (2.17), one has

$$(h_q) = -qP_{(a,b)} + \sum_{\xi^{q+1}=1,\ \xi \neq 1} P_{(a,\xi b)},$$

implying that $q \in H(P_{(a,b)})$. □

Theorem 4.4. *Let $P_{(a,b)} \in \mathcal{X}_3(\mathbb{F}_{q^2}) \setminus \mathcal{O}$ be a point such that $\alpha(P_{(a,b)})^2 - \alpha(P_{(a,b)}) + 1 = 0$. Then*

$$H(P_{(a,b)}) = \langle q, q+1, (q-1) + i(q-2) \mid i = 0, \dots, m-2 \rangle.$$

Proof. We start by showing that the semigroup $H := \langle q, q+1, (q-1) + i(q-2) \mid i = 0, \dots, m-2 \rangle$ is contained in $H(P_{(a,b)})$. To this aim, we show that $q, q+1, (q-1)+i(q-2)$, for all $i = 0, \dots, m-2$, are pole numbers of P. By Lemma 4.3, we already know that $q, q+1 \in H(P_{(a,b)})$, so we are left to show that $(q-1) + i(q-2)$ is a pole number for every $i = 0, \dots, m-2$. We prove this considering the following family of functions. For all i such that $0 \leq i \leq m-2$, let $P_{(\bar{a},0)}$ be a point such that $\bar{a}^m + 1 = 0$ and define the function

$$G_i := \frac{g_i \cdot f^{i+1}_{P_{(\bar{a},0)},1}}{f^{i+1}_{P_{(a,b)},1} \cdot (x-\bar{a})^{i+1}},$$

where the functions g_i are those built in Theorem 3.19. Then using equations (2.8), (2.16), (2.17) and Theorem 3.19, the divisor of the function G_i is seen to be

$$(G_i) = E_i - ((q-1) + i(q-2))P_{(a,b)},$$

where $E_i \in \text{Div}(\mathcal{X}_3)$ is an effective divisor such that $P_{(a,b)} \notin \text{supp}(E_i)$. Therefore, $(q-1) + i(q-2) \in H(P_{(a,b)})$ for all $i = 1, \dots, m-2$.

To complete the proof, we need to show that the genus of the semigroup H is less than or equal to $g(\mathcal{X}_3)$. Indeed the inequality $g(H) \geq g(\mathcal{X}_3)$ is already clear, since we just showed that $H \subseteq H(P_{(a,b)})$. Of course we know $0 \in H$, but we claim that for $j = 1, \dots, m-1$, all integers in $\{j(q-2)+1, \dots, j(q+1)\}$ are in H as well. This is clear for $j = 1$, since $q-1, q, q+1 \in H$. If this is true for some $j < m-1$, then adding $q-1$ and

$q+1$ to all integers in $\{j(q-2)+1,\dots,j(q+1)\}$, shows that the consecutive integers in $\{(j+1)(q-2)+2,\dots,(j+1)(q+1)\}$ are all in H. Since $(j+1)(q-2)+1 = (q-1)+j(q-2) \in H$, we conclude that all integers in $\{(j+1)(q-2)+1,\dots,(j+1)(q+1)\}$ are in H. This shows the claim. Now note that $\{(m-1)(q-2)+1,\dots,(m-1)(q+1)\}$ consists of $q-2$ consecutive integers, all in H. Adding integral multiples of $q-1$ and q to this set, we obtain that all integers greater than or equal to $(m-1)(q-2)+1+q-1 = (m-1)(q+1)+2$ are in H. This means that the number of gaps in H is at most

$$g(H) \le (q-2)+(q-5)+\dots+3+1.$$

The final $+1$ counts the potential gap $(m-1)(q+1)+1$. Hence

$$g(H) \le 1+3\sum_{k=1}^{m-1} k = 1+3m(m-1)/2 = g(\mathcal{X}_3),$$

which is what we needed to show. □

Theorem 4.5. *Let $P_{(a,b)} \in \mathcal{X}_3(\mathbb{F}_{q^2}) \setminus \mathcal{O}$ be a point such that $\alpha(P_{(a,b)})^2 - \alpha(P_{(a,b)}) + 1 \neq 0$. Further, let i be the $\mathcal{P}$-order of $\alpha(P_{(a,b)})$. If $i \le m-2$, then*

$$H(P_{(a,b)}) = \langle q, q+1, (q-1)+j(q-2), (q-1)+i(q-2)-1 \mid j=0,\dots,i-1\rangle.$$

If $i = m-1$, then

$$H(P_{(a,b)}) = \langle q, q+1, (q-1)+j(q-2) \mid j=0,\dots,m-2\rangle.$$

Proof. We first assume that $i \le m-2$. We proceed similarly as in the proof of Theorem 4.4, showing that the semigroup $H := \langle q-1, q, q+1, (q-1)+j(q-2), (q-1)+i(q-2)-1 \mid j=1,\dots,i-1\rangle$ is contained in $H(P_{(a,b)})$ and has at most $g(\mathcal{X}_3)$ gaps. For all j such that $j=1,\dots,i-1$, let $P_{(\bar{a},0)}$ be a point with $\bar{a}^m+1=0$ and define the function

$$F_j := \frac{f_j \cdot f_{P_{(\bar{a},0)},1}^{j+1}}{f_{P_{(a,b)},1}^{j+1} \cdot (x-\bar{a})^{j+1}},$$

where the f_j are the functions built in Theorem 3.12. Using equations (2.8), (2.16), (2.17) and Theorem 3.19, the divisor of the function F_j can be seen to be

$$(F_j) = E_j - ((q-1)+j(q-2))P_{(a,b)}$$

where $E_j \in \mathrm{Div}(\mathcal{X}_3)$ is an effective divisor such that $P_{(a,b)} \notin \mathrm{supp}(E_j)$. Therefore, $(q-1)+j(q-2) \in H(P)$ for all $j=1,\dots,i-1$. Similarly

$$(F_i) = E_i - ((q-1)+i(q-2)-1)P_{(a,b)},$$

where $E_i \in \mathrm{Div}(\mathcal{X}_3)$ is an effective divisor such that $P_{(a,b)} \notin \mathrm{supp}(E_i)$. Hence, we now have shown that $H \subseteq H(P_{(a,b)})$.

What remains to be shown is that the genus of the semigroup H does not exceed $g(\mathcal{X}_3)$. We know $0 \in H$ and just as in the proof of Theorem 4.4 we conclude that all integers in the set $\{j(q-2)+1, \dots, j(q+1)\}$ are in H for any $j = 1, \dots, i$. Further, we have already shown that $(i+1)(q-2) \in H$ and adding $q-1$, q, and $q+1$ to the integers in $\{i(q-2)+1, \dots, i(q+1)\}$ yields that $\{(i+1)(q-2)+2, \dots, (i+1)(q+1)\} \subseteq H$.

Since $P_{(a,b)} \in \mathcal{X}_3(\mathbb{F}_{q^2})$, Lemma 3.11 implies that $i+1$ divides m. We claim that for $k = 0, \dots, m/(i+1)-1$ and all $j = 1, \dots, i$ the sets $\{(k(i+1)+j)(q-2)+1, \dots, (k(i+1)+j)(q+1)\}$ are contained in H as well as the integer $((k+1)(i+1))(q-2)$ and the set $\{(k+1)(i+1)(q-2)+2, \dots, (k+1)(i+1)(q+1)\}$. We have so far shown this for $k = 0$. If the claim is true for some $k-1 < m/(i+1)-1$, adding $(i+1)(q-2)$ and the integers in $\{(i+1)(q-2)+2, \dots, (i+1)(q+1)\}$, immediately shows that the claim is true for k as well. This proves the claim. For $k = m/(i+1)-1$, we obtain that $\{m(q-2)+2, \dots, m(q+1)\}$, which contains q consecutive integers, is a subset of H. This shows that all integers greater than or equal to $m(q-2)+2 = (m-1)(q+1)+2$ are in H. Estimating the number of gaps is now done very similarly as in the proof of Theorem 4.4. The number of gaps of the semigroup there is in fact exactly the same as those of the semigroup H constructed here: in the proof of Theorem for all $k = 1, \dots, m/(i+1)-1$, the integer $k(i+1)(q-2)$ was a gap, while $k(i+1)(q-2)+1$ was not, while now $k(i+1)(q-2)$ is in H and $k(i+1)(q-2)+1$ is not. Hence $g(H) \leq g(\mathcal{X}_3)$ again holds.

We are left to prove the theorem if $i = m-1$. Using exactly the same approach as above, we can show that $H := \langle q-1, q, q+1, (q-1)+j(q-2) \mid j = 1, \dots, m-2 \rangle$ is contained in $H(P_{(a,b)})$. Now note that H is exactly the same semigroup as the one occurring in Theorem 4.4. Hence $g(H) \leq g(\mathcal{X}_3)$ holds in this case as well. □

4.3. Some remarks on rational Weierstrass points

From the previous two subsections, we have a complete determination of all types of Weierstrass semigroups that occur among them and how many points attain a given type. To avoid trivial cases, we assume $q \geq 5$.

Theorem 4.6. *The number of distinct Weierstrass semigroups $H(P)$ among $P \in \mathcal{X}_3(\mathbb{F}_{q^2})$ is exactly the same as the number of divisors of m. The semigroups that occur and the $P \in \mathcal{X}_3(\mathbb{F}_{q^2})$ for which they occur are:*

- *$H(P) = \langle q-2, q, q+1 \rangle$ for $q+1$ many $P \in \mathcal{O}$.*
- *$H(P) = \langle q, q+1, (q-1)+j(q-2), (q-1)+i(q-2)-1 \mid j = 0, \dots, i-1 \rangle$, where $1 \leq i \leq m-2$ and $i+1$ divides m, for the $(q+1)^2\varphi(i+1)$ many $P \in \mathcal{X}_3(\mathbb{F}_{q^2})$ for which $\alpha(P)$ has $\mathcal{P}$-order i.*

- *$H(P) = \langle q, q+1, (q-1)+j(q-2) \mid j = 0, \dots, m-2\rangle$ for the $(q+1)^2\varphi(m)$ many $P \in \mathcal{X}_3(\mathbb{F}_{q^2})$ for which $\alpha(P)$ has $\mathcal{P}$-order $m-1$ as well as for the $2m(q+1)$ many $P \in \mathcal{X}_3(\mathbb{F}_{q^2})$ for which $\alpha(P)^2 - \alpha(P) + 1 = 0$.*

Proof. First of all, Theorems 4.2, 4.4 and 4.5 combined describe all possible Weierstrass semigroups that occur among $P \in \mathcal{X}_3(\mathbb{F}_{q^2})$. Lemma 3.11 implies that the only possible $\mathcal{P}$-orders i for $P \in \mathcal{X}_3(\mathbb{F}_{q^2})$ correspond to divisors $i+1 \geq 2$ of m. Therefore the total number of possible Weierstrass semigroups is exactly the number of divisors of m, where the divisor 1 counts the semigroup $\langle q-2, q, q+1\rangle$.

As for the number of $P \in \mathcal{X}_3(\mathbb{F}_{q^2})$ attaining one particular type: we know that $|\mathcal{O}| = q+1$, while Lemma 3.11 implies how many P have $\mathcal{P}$-order equal to a given i. The only number of points left to determine is those $P_{(a,b)} \in \mathcal{X}_3(\mathbb{F}_{q^2})$ such that $\alpha(P_{(a,b)})^2 - \alpha(P_{(a,b)})+1 = 0$. Using that $\alpha(P_{(a,b)}) = a^m/(1+a^m)$, we see that $\alpha(P_{(a,b)})^2 - \alpha(P_{(a,b)})+1 = 0$ if and only if $a^{2m}+a^m+1 = 0$ and $b^{q+1} = -1$. Hence, for exactly $2m(q+1)$ many $P_{(a,b)} \in \mathcal{X}_3(\mathbb{F}_{q^2})$ one has $\alpha(P_{(a,b)})^2 - \alpha(P_{(a,b)}) + 1 = 0$. □

Remark 4.7. It is not hard to see that the indicated generators in Theorem 4.6 are in all cases a minimal set of generators. Since $\mathcal{X}_3$ is a maximal curve over $\mathbb{F}_{q^2}$, its number of $\mathbb{F}_{q^2}$-rational points is equal to $q^2+1+2qg(\mathcal{X}_3) = \frac{(q+1)(q^2+q+3)}{3}$. Note as a sanity check that indeed,

$$q+1+\sum_{i=1;i+1|m}^{m-1}(q+1)^2\varphi(i+1)+2m(q+1) = q^2+1+2qg(\mathcal{X}_3),$$

using the equation $\sum_{d|m}\varphi(d) = m$ where the sum is over all divisors of m.

Also the multiplicity (i.e., the smallest positive element) of the semigroups is easy to determine using Theorem 4.6: it is $q-1$, unless $P \in \mathcal{O}$ in which case it is $q-2$. Another parameter of a numerical semigroup is its conductor c. This is the smallest nonnegative integer c such that $\mathbb{Z}_{\geq c}$ is contained in the semigroup. Since $(q-2)D_\infty$ is a canonical divisor by Lemma 2.23, $3D_\infty \sim (q+1)P_{(a,0)}$ by equation (2.16), and for any $P \in \mathcal{X}_3(\mathbb{F}_{q^2})$ by the Fundamental Equation $(q+1)P \sim (q+1)P_{(a,0)}$, we see that $(q-2)mP$ is a canonical divisor for all $P \in \mathcal{X}_3(\mathbb{F}_{q^2})$. This implies that $H(P)$ is symmetric for all $P \in \mathcal{X}_3(\mathbb{F}_{q^2})$. In particular the largest gap in $H(P)$ is $2g(\mathcal{X}_3)-1$ for all $P \in \mathcal{X}_3(\mathbb{F}_{q^2})$, implying that the conductor of $H(P)$ is $2g(\mathcal{X}_3)$.

5. Weierstrass semigroups at the non-$\mathbb{F}_{q^2}$-rational points of $\mathcal{X}_3$

In this section, we compute the Weierstrass semigroups at all the remaining points of $\mathcal{X}_3$, namely at all the non-$\mathbb{F}_{q^2}$-rational points. We start by computing the semigroup for the generic case, i.e., for the non-Weierstrass points of the curve and, finally, we determine the semigroups for the non-$\mathbb{F}_{q^2}$-rational Weierstrass points.

5.1. The generic case

Theorem 5.1. *Let $P_{(a,b)} \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \setminus \mathcal{X}_3(\mathbb{F}_{q^2})$ such that $\mathcal{P}_j(\alpha) \neq 0$ for all $j = 2, \dots, m-1$. Then*

$$G(P_{(a,b)}) = \{jq + k \mid j = 0, \dots, m-2,\ k = 1, \dots, q-3j-2\} \cup \{(m-1)q+1\},$$

that is

$$H(P_{(a,b)}) = \{0, (j+1)(q-3)+2+k, (m-1)q+2, \dots \mid j = 0, \dots, m-2,\ k = 0, \dots, 3j+1\}.$$

Proof. Let $\Gamma := \{jq+k \mid j = 0, \dots, m-2,\ k = 1, \dots, q-3j-2\} \cup \{(m-1)q+1\}$ be the putative set of gaps. Direct computations show that $|\Gamma| = 1 + \sum_{j=0}^{m-2}(q-(3j+2)) = g(\mathcal{X}_3)$.

We need to prove that, for every $g \in \Gamma$, there exists a function $h_g \in L((q-2)D_\infty)$ such that $v_P(h_g) = g - 1$.

Let $g = jq + k \in \Gamma$. We distinguish the following cases.

(1) If $\lfloor \frac{k}{3} \rfloor \neq 0$, then we define:

$$h_g := \begin{cases} F^j_{P_{(a,b)}} \cdot f_{\lfloor \frac{k}{3} \rfloor - 1} & \text{if } k \equiv 0 \pmod 3, \\ F^j_{P_{(a,b)}} \cdot (y-b) \cdot f_{\lfloor \frac{k}{3} \rfloor - 1} & \text{if } k \equiv 1 \pmod 3, \\ F^j_{P_{(a,b)}} \cdot t_{P_{(a,b)}} \cdot f_{\lfloor \frac{k}{3} \rfloor - 1} & \text{if } k \equiv 2 \pmod 3. \end{cases}$$

(2) If $\lfloor \frac{k}{3} \rfloor = 0$, we define instead:

$$h_g := \begin{cases} F^j_{P_{(a,b)}} & \text{if } k = 1, \\ F^j_{P_{(a,b)}} \cdot (y-b) & \text{if } k = 2. \end{cases}$$

Here, the function $f_{\lfloor \frac{k}{3} \rfloor - 1}$ is one of the functions f_i constructed in Theorem 3.12 and the function $F_{P_{(a,b)}}$ is as defined in equation (2.21).

Note that, as $j = 0, \dots, m-2$, for $k = 3, \dots, q-3j-2$ it holds that

$$0 \leq \left\lfloor \frac{k}{3} \right\rfloor - 1 \leq \left\lfloor \frac{q-3j-2}{3} \right\rfloor - 1 = \frac{q-2}{3} - j - 1 = m - 2 - j \leq m-2,$$

hence the function h_g is well-defined, for any $i = 0, \dots, m-2$ and $k = 1, \dots, q-3j-2$. Indeed, defining the function h_g in this way, for any $g = jq + k \in \Gamma$, we have what follows.

Case 1: $\lfloor \frac{k}{3} \rfloor \neq 0$.

If $k \equiv 0 \pmod 3$, then

$$v_P(h_g) = jq + 3\left(\left\lfloor \frac{k}{3} \right\rfloor - 1\right) + 2 = jq + k - 1$$

and

$$(h_g)_\infty \leq \left(3j + 3\left(\left\lfloor \frac{k}{3} \right\rfloor - 1 + 1\right)\right) D_\infty = (3j{+}k)D_\infty \leq (3j{+}q{-}3j{-}2)D_\infty = (q{-}2)D_\infty.$$

If $k \equiv 1 \pmod 3$, then

$$v_P(h_g) = jq + 3\left(\left\lfloor \frac{k}{3} \right\rfloor - 1\right) + 2 + 1 = jq + (k-1) - 3 + 3 = jq + k - 1$$

and

$$\begin{aligned}(h_g)_\infty &\leq \left(3j + 3\left(\left\lfloor \frac{k}{3} \right\rfloor - 1 + 1\right) + 2\right) D_\infty = (3j + k + 1)D_\infty \\ &\leq (3j + q - 3j - 4 + 1)D_\infty = (q-3)D_\infty,\end{aligned}$$

where the last inequality follows from the fact that $q - 3j - 2 \equiv 0 \pmod 3$, hence if $k \equiv 1 \pmod 3$, then $k \leq (q - 3j - 2) - 2 = q - 3j - 4$.

If $k \equiv 2 \pmod 3$, then

$$v_P(h_g) = jq + 3\left(\left\lfloor \frac{k}{3} \right\rfloor - 1\right) + 2 + 2 = jq + (k-2) - 3 + 4 = jq + k - 1$$

and

$$\begin{aligned}(h_g)_\infty &\leq \left(3j + 3\left(\left\lfloor \frac{k}{3} \right\rfloor - 1 + 1\right) + 3\right) D_\infty = (3j + k + 1)D_\infty \\ &\leq (3j + q - 3j - 3 + 1)D_\infty = (q-2)D_\infty,\end{aligned}$$

where the last inequality follows from the fact that $q - 3j - 2 \equiv 0 \pmod 3$, hence if $k \equiv 2 \pmod 3$, then $k \leq (q - 3j - 2) - 1 = q - 3j - 3$.

Case 2: $\left\lfloor \frac{k}{3} \right\rfloor = 0$.

If $k = 1$, then

$$v_P(h_g) = jq$$

and

$$(h_g)_\infty \leq (3j)D_\infty \leq ((q+1) - 6)D_\infty = (q-5)D_\infty.$$

If $k = 2$, then

$$v_P(h_g) = jq + 1$$

and

$$(h_g)_\infty \leq (3j + 2)D_\infty \leq ((q + 1) - 6 + 2)D_\infty = (q - 3)D_\infty. \quad \square$$

Since the Weierstrass semigroup at all but a finite number of points of $\mathcal{X}_3$ is as described in Theorem 5.1, we call

$$H_{gen} := \{0, (j + 1)(q - 3) + 2 + k, (m - 1)q + 2, \dots \mid j = 0, \dots, m - 2,\ k = 0, \dots, 3j + 1\}$$

the *generic* Weierstrass semigroup of $\mathcal{X}_3$ and

$$G_{gen} := \{jq + k \mid j = 0, \dots, m - 2,\ k = 1, \dots, q - 3j - 2\} \cup \{(m - 1)q + 1\}$$

the *generic* set of gaps of $\mathcal{X}_3$.

5.2. The Weierstrass semigroups at the non-$\mathbb{F}_{q^2}$-rational Weierstrass points

Theorem 5.2. *Let $P_{(a,b)} \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \setminus \mathcal{X}_3(\mathbb{F}_{q^2})$ and i the $\mathcal{P}$-order of $\alpha(P_{(a,b)})$. Suppose that $i \leq m - 2$. Then*

$$G(P_{(a,b)}) = \left(G_{gen} \setminus \left\{(m - 2 - i - \ell(i + 1))q + (\ell + 1)(3i + 3) \,|\, \ell = 0, \dots, \left\lfloor \frac{m - 2 - i}{i + 1} \right\rfloor \right\}\right) \\ \cup \left\{(m - 2 - i - \ell(i + 1))q + (\ell + 1)(3i + 3) + 1 \mid \ell = 0, \dots, \left\lfloor \frac{m - 2 - i}{i + 1} \right\rfloor \right\}, \tag{5.3}$$

that is

$$H(P_{(a,b)}) = \\ = \left(H_{gen} \setminus \left\{(m - 2 - i - \ell(i + 1))q + (\ell + 1)(3i + 3) + 1 \mid \ell = 0, \dots, \left\lfloor \frac{m - 2 - i}{i + 1} \right\rfloor \right\}\right) \\ \cup \left\{(m - 2 - i - \ell(i + 1))q + (\ell + 1)(3i + 3) \mid \ell = 0, \dots, \left\lfloor \frac{m - 2 - i}{i + 1} \right\rfloor \right\}.$$

Proof. Let G as in equation (5.3) be the putative set of gaps. Since the cardinality of the set

$$\left\{(m - 2 - i - \ell(i + 1))q + (\ell + 1)(3i + 3) \mid \ell = 0, \dots, \left\lfloor \frac{m - 2 - i}{i + 1} \right\rfloor \right\}$$

is the same as the cardinality of the set

$$\left\{(m-2-i-\ell(i+1))q+(\ell+1)(3i+3)+1 \mid \ell=0,\dots,\left\lfloor\frac{m-2-i}{i+1}\right\rfloor\right\},$$

it follows immediately that $|G(P_{(a,b)})| = |G_{gen}| = g(\mathcal{X}_3)$. Hence, as in the proof of Theorem 5.1, we are now left to show that, for each $g \in G$, there exists a function h_g such that $h_g \in L((q-2)D_\infty)$ and $v_P(h_g) = g-1$.

For any $g = jq+k$, let $\mathfrak{c} := \left\lfloor\frac{k}{3(i+1)}\right\rfloor$. We can then write

$$\left\lfloor\frac{k}{3}\right\rfloor = \mathfrak{c}(i+1)+h,$$

where h is an integer such that $0 \le h \le i$, and

$$k = \left\lfloor\frac{k}{3}\right\rfloor \cdot 3 + r = 3\mathfrak{c}(i+1)+3h+r,$$

where r is an integer such that $0 \le r \le 2$. First note that, with this choice of $\mathfrak{c}$, $0 \le \lfloor\frac{k}{3}\rfloor - (\mathfrak{c}(i+1)+1) \le i-1$ for all k such that $\lfloor\frac{k}{3}\rfloor \ne \mathfrak{c}(i+1)$. Indeed,

$$\left\lfloor\frac{k}{3}\right\rfloor - (\mathfrak{c}(i+1)+1) \le i-1 \quad\Longleftrightarrow\quad \left\lfloor\frac{k}{3}\right\rfloor - \mathfrak{c} \le i+\mathfrak{c}i,$$

hence, as $\lfloor\frac{k}{3}\rfloor = \mathfrak{c}(i+1)+h$, with h an integer such that $0 \le h \le i$, we obtain

$$\left\lfloor\frac{k}{3}\right\rfloor - \mathfrak{c} \le i+\mathfrak{c}i \quad\Longleftrightarrow\quad \mathfrak{c}(i+1)+h-\mathfrak{c} \le i+\mathfrak{c}i \quad\Longleftrightarrow\quad h \le i,$$

which is satisfied.

We now distinguish the following cases.

(1) If $\lfloor\frac{k}{3}\rfloor \ne \mathfrak{c}(i+1)$, then we define:

$$h_g := \begin{cases} F^j_{P_{(a,b)}} \cdot f_{\lfloor\frac{k}{3}\rfloor-(\mathfrak{c}(i+1)+1)} \cdot f_i^{\mathfrak{c}} & \text{if } k \equiv 0 \pmod 3,\\ F^j_{P_{(a,b)}} \cdot (y-b) \cdot f_{\lfloor\frac{k}{3}\rfloor-(\mathfrak{c}(i+1)+1)} \cdot f_i^{\mathfrak{c}} & \text{if } k \equiv 1 \pmod 3,\\ F^j_{P_{(a,b)}} \cdot t_{P_{(a,b)}} \cdot f_{\lfloor\frac{k}{3}\rfloor-(\mathfrak{c}(i+1)+1)} \cdot f_i^{\mathfrak{c}} & \text{if } k \equiv 2 \pmod 3.\end{cases}$$

(2) If $\lfloor \frac{k}{3} \rfloor = \mathfrak{c}(i+1)$, we define instead:

$$h_g := \begin{cases} F^j_{P_{(a,b)}} \cdot (y-b) \cdot t_{P_{(a,b)}} \cdot f_{i-1} \cdot f_i^{\mathfrak{c}-1} & \text{if } k \equiv 0 \pmod 3 \text{ and } j \leq m-2-i, \\ F^j_{P_{(a,b)}} \cdot f_{\frac{k}{3}-1} & \text{if } k \equiv 0 \pmod 3 \text{ and } j \geq m-1-i, \\ F^j_{P_{(a,b)}} \cdot f_i^{\mathfrak{c}} & \text{if } k \equiv 1 \pmod 3, \\ F^j_{P_{(a,b)}} \cdot (y-b) \cdot f_i^{\mathfrak{c}} & \text{if } k \equiv 2 \pmod 3. \end{cases}$$

Indeed, for $g = jq + k \in G$, we have the following situation.
Case 1: $\lfloor \frac{k}{3} \rfloor \neq \mathfrak{c}(i+1)$.

If $k \equiv 0 \pmod 3$, then

$$v_{P_{(a,b)}}(h_g) = jq + 3\left(\left\lfloor \frac{k}{3} \right\rfloor - (\mathfrak{c}(i+1)+1)\right) + 2 + 3\mathfrak{c}(i+1) = jq + k - 3 + 2 = jq + k - 1$$

and

$$\begin{aligned}(h_g)_\infty &\leq (3j + 3\left(\left\lfloor \frac{k}{3} \right\rfloor - (\mathfrak{c}(i+1)+1) + 1\right) + 3\mathfrak{c}(i+1))D_\infty \\ &= (3j+k)D_\infty \\ &\leq (3j + q - 3j - 2)D_\infty = (q-2)D_\infty,\end{aligned}$$

where the last inequality above follows from the fact that $k \leq q - 3j - 2$.

If $k \equiv 1 \pmod 3$, then

$$v_{P_{(a,b)}}(h_g) = jq + 1 + 3\left(\left\lfloor \frac{k}{3} \right\rfloor - (\mathfrak{c}(i+1)+1)\right) + 2 + 3\mathfrak{c}(i+1) = jq + (k-1) - 3 + 3 = jq + k - 1$$

and

$$\begin{aligned}(h_g)_\infty &\leq (3j + 2 + 3\left(\left\lfloor \frac{k}{3} \right\rfloor - (\mathfrak{c}(i+1)+1) + 1\right) + 3\mathfrak{c}(i+1))D_\infty \\ &= (3j+k+1)D_\infty \\ &\leq (3j + q - 3j - 3)D_\infty = (q-3)D_\infty,\end{aligned}$$

where the last inequality follows from the fact that $q - 3j - 2 \equiv 0 \pmod 3$, hence if $k \equiv 1 \pmod 3$, then $k \leq (q - 3j - 2) - 2 = q - 3j - 4$.

If $k \equiv 2 \pmod 3$, then

$$v_{P_{(a,b)}}(h_g) = jq + 2 + 3\left(\left\lfloor \frac{k}{3} \right\rfloor - (\mathfrak{c}(i+1)+1)\right) + 2 + 3\mathfrak{c}(i+1) = jq + (k-2) - 3 + 4 = jq + k - 1$$

and

$$\begin{aligned}(h_g)_\infty &\leq (3j+3+3\left(\left\lfloor\frac{k}{3}\right\rfloor-(\mathfrak{c}(i+1)+1)+1\right)+3\mathfrak{c}(i+1))D_\infty\\ &=(3j+k+1)D_\infty\\ &\leq(3j+q-3j-2)D_\infty=(q-2)D_\infty,\end{aligned}$$

where the last inequality follows from the fact that $q-3j-2\equiv 0 \pmod 3$, hence if $k\equiv 2 \pmod 3$, then $k\leq(q-3j-2)-1=q-3j-3$.

Case 2: $\left\lfloor\frac{k}{3}\right\rfloor=\mathfrak{c}(i+1)$.

If $k\equiv 0 \pmod 3$ and $j\leq m-2-i$, then

$$v_{P_{(a,b)}}(h_g)=jq+1+2+3(i-1)+2+3(\mathfrak{c}-1)(i+1)=jq+3\mathfrak{c}(i+1)-1=jq+k-1$$

and

$$\begin{aligned}(h_g)_\infty &\leq(3j+2+3+3i+3(\mathfrak{c}-1)(i+1))D_\infty\\ &=(3j+k+2)D_\infty\\ &\leq(3j+q-3j-5+2)D_\infty=(q-3)D_\infty,\end{aligned}$$

since in this case $k\leq q-3j-3\equiv 2 \pmod 3$ and hence, as $k\equiv 0 \pmod 3$, then $k\leq(q-3j-3)-2=q-3j-5$.

If $k\equiv 0 \pmod 3$ and $j\geq m-1-i$, then note that, as $3j\geq q-3i-2$, then $k\leq q-3j-2\leq q-(q-3i-2)-2=3i$ and $\frac{k}{3}-1\leq i-1$. Hence, we have that

$$v_{P_{(a,b)}}(h_g)=jq+3\left(\frac{k}{3}-1\right)+2=jq+k-1$$

and

$$\begin{aligned}(h_g)_\infty &\leq(3j+3\left(\frac{k}{3}\right))D_\infty\\ &=(3j+k)D_\infty\\ &\leq(3j+q-3j-2)D_\infty=(q-2)D_\infty,\end{aligned}$$

since $k\leq q-3j-2$ in this case. If $k\equiv 1 \pmod 3$, then

$$v_{P_{(a,b)}}(h_g)=jq+3\mathfrak{c}(i+1)=jq+k-1$$

as $3\left\lfloor\frac{k}{3}\right\rfloor=3\mathfrak{c}(i+1)=k-1$. Moreover,

$$\begin{aligned}(h_g)_\infty &\le (3j+3\mathfrak{c}(i+1))D_\infty\\ &= (3j+k-1)D_\infty\\ &\le (3j+q-3j-2-1)D_\infty = (q-3)D_\infty,\end{aligned}$$

since $k \le q-3j-2$.

If $k \equiv 2 \pmod 3$, then

$$v_{P_{(a,b)}}(h_g) = jq+1+3\mathfrak{c}(i+1) = jq+(k-2)+1 = jq+k-1$$

as $3\left\lfloor \frac{k}{3}\right\rfloor = 3\mathfrak{c}(i+1) = k-2$. Moreover,

$$\begin{aligned}(h_g)_\infty &\le (3j+2+3\mathfrak{c}(i+1))D_\infty\\ &= (3j+k)D_\infty\\ &\le (3j+q-3j-2)D_\infty = (q-2)D_\infty,\end{aligned}$$

since $k \le q-3j-2$. □

5.3. Final remarks on the Weierstrass points of $\mathcal{X}_3$

We finish this section by collecting a few further facts on the Weierstrass points of $\mathcal{X}_3$.

Proposition 5.4. *Only for $q \in \{2,5,8\}$ are all Weierstrass points of $\mathcal{X}_3$ defined over $\mathbb{F}_{q^2}$.*

Proof. Lemma 3.11 and Theorem 5.2 imply that a non-rational Weierstrass point exists precisely if there exists i such that $1 \le i \le m-2$, $\gcd(i+1,p)=1$, and $i+1$ does not divide m. Since m has at most $m/3+1$ divisors (not counting m itself) and there are at most $\lfloor m/p \rfloor$ multiples of p between 1 and m, we see that a non-rational Weierstrass point exists if $m-2 > 1+m/3+m/p$. Since $p \ge 2$, and $m-2 > 1+m/3+m/2$ if and only if $q > 53$, this already shows that there exists a non-rational Weierstrass point for all $q > 53$. It is trivial to check that i satisfying the conditions exists for $q \in \{11,17,23,29,32,41,47,53\}$, while no such i exists for $i \in \{2,5,8\}$. □

Remark 5.5. It is at this point quite simple to determine the number of distinct possible Weierstrass semigroups $H(P)$ as P varies. Indeed, the possible $\mathcal{P}$-orders less than or equal to $m-1$ are simply the number of i between 1 and $m-1$, such that $\gcd(p,i+1)=1$. Counting the semigroup for $P \in \mathcal{O}$ as well, this gives $m - \lfloor m/p \rfloor$ possible semigroups different from the generic semigroup. The generic semigroup corresponds to those points P on $\mathcal{X}_3$ whose $\mathcal{P}$-order is at least m. Hence there are precisely $m - \lfloor m/p \rfloor + 1$ possible semigroups.

Remark 5.6. For $\mathbb{F}_{q^2}$-rational points, we determined the multiplicity and conductors the corresponding Weierstrass semigroups. Using Theorem 5.1, we see that in the generic case, the smallest positive non-gap in $H(P)$ is $q-1$, while the largest gap is $(m-1)q+1$. Hence in the generic case, the multiplicity is $q-1$ and the conductor $(m-1)q+2$. If $P \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \setminus \mathcal{X}_3(\mathbb{F}_{q^2})$ has $\mathcal{P}$-order $i \le m-2$, then Theorem 5.2 implies quite easily that the largest gap still is $(m-1)q+1$ and therefore that the conductor is $(m-1)q+2$.

The situation for the multiplicity is more complicated. We show what is going on in the following theorem.

Theorem 5.7. *Let $P_{(a,b)} \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \setminus \mathcal{X}_3(\mathbb{F}_{q^2})$. Then the multiplicity of the semigroup $H(P_{(a,b)})$ is $q-2$ or $q-1$. Moreover, the following are equivalent:*

(1) The multiplicity of $H(P_{(a,b)})$ is $q-2$.
(2) The $\mathcal{P}$-order i of $\alpha(P_{(a,b)})$ is such that $i+1$ divides $m-1$.
(3) $\mathcal{P}_{m-1}(\alpha(P_{(a,b)}))=0$.
(4) The Frobenius of (a,b), that is $\Phi(a,b) := (a^{q^2}, b^{q^2})$, lies on the tangent line of the plane curve $y^{q+1}+x^{2m}+x^m=0$ at (a,b).

Proof. Comparing the gap set in the generic case and the case described in Theorem 5.2, we see that the only difference is that the value of certain gaps is increased by one. Since in the generic case, $1,\dots,q-2$ are gaps and $q-1$ is not a gap, this means that the multiplicity of $H(P_{(a,b)})$ for any $P_{(a,b)} \in \mathcal{X}_3(\overline{\mathbb{F}}_{q^2}) \setminus \mathcal{X}_3(\mathbb{F}_{q^2})$ can be either $q-2$ or $q-1$. Now we show equivalence of the four listed items. For convenience, we write $P = P_{(a,b)}$ and $\alpha = \alpha(P_{(a,b)})$.

(1) ⇒ (2): Assume that $q-2 \in H(P)$ and let i be the $\mathcal{P}$-order of α. Then according to Theorem 5.2 $q-2$ can be written in the form $(m-2-i-\ell(i+1))q+(\ell+1)(3i+3)$ for some ℓ between 0 and $\lfloor (m-2-i)/(i+1) \rfloor$. Then necessarily $m-2-i-\ell(i+1)=0$, which is only possible if $\ell=(m-2-i)/(i+1)$ is an integer. Hence $i+1$ divides $m-1$.

(2) ⇒ (3): From the definition of the polynomial $\mathcal{P}_{i+1}(s)$, we see that $((\alpha+\zeta_3)/(\alpha+\zeta_3^2))^{i+1}=1$. If $i+1$ divides $m-1$, this implies that $((\alpha+\zeta_3)/(\alpha+\zeta_3^2))^{m-1}=1$, which in turn implies that $\mathcal{P}_{m-1}(\alpha)=0$.

(3) ⇒ (4): The tangent line ℓ_P of the plane curve $y^{q+1}+x^{2m}+x^m=0$ at (a,b) is given by the equation $a^{m-1}(2a^m+1)(x-a)+3b^q(y-b)=0$. Hence $\Phi(a,b)$ lies on ℓ_P if and only if $a^m(2a^m+1)(a^{q^2-1}-1)+3b^{q+1}(b^{q^2-1}-1)=0$. Using that $b^{q+1}=-a^{2m}-a^m$, we can express all quantities in this equation in terms of a^m and obtain the equivalent equation $a^m((a^m)^{q-1}-1)^2(2(a^m)^q+(a^m)^{q-1}+a^m+2)=0$. Since $P \notin \mathcal{X}_3(\mathbb{F}_{q^2})$, we know $a^m \notin \mathbb{F}_q$ and hence we conclude that

$$(a^{q^2}, b^{q^2}) \in \ell_P \Leftrightarrow 2(a^m)^q+(a^m)^{q-1}+a^m+2=0.$$

Using that $a^m = \alpha/(1-\alpha)$, we conclude that

$$(a^{q^2}, b^{q^2}) \in \ell_P \Leftrightarrow \alpha^{q-1}+(\alpha-1)^{q-1}+1=0. \qquad (5.8)$$

Now let us investigate our assumption: $\mathcal{P}_{m-1}(\alpha) = 0$. This implies

$$\left(\frac{\alpha+\zeta_3}{\alpha+\zeta_3^2}\right)^{q-2} = 1 \text{ and hence } \left(\frac{\alpha+\zeta_3}{\alpha+\zeta_3^2}\right)^{q} = \left(\frac{\alpha+\zeta_3}{\alpha+\zeta_3^2}\right)^{2},$$

which in turn gives

$$0 = (\alpha+\zeta_3)^q(\alpha+\zeta_3^2)^2 - (\alpha+\zeta_3^2)^q(\alpha+\zeta_3)^2 = (\alpha^q+\zeta_3^2)(\alpha+\zeta_3^2)^2 - (\alpha^q+\zeta_3)(\alpha+\zeta_3)^2.$$

Multiplying everything out and dividing by $\zeta_3^2 - \zeta_3$, we find that

$$0 = 2\alpha^{q+1} - \alpha^q + \alpha^2 - 2\alpha = \alpha(\alpha-1)(\alpha^{q-1} + (\alpha-1)^{q-1} + 1).$$

In light of equation (5.8), we obtain that $\Phi(a,b) \in \ell_P$.

(4) ⇒ (1): If $\Phi(a,b) \in \ell_P$, then the function t_P/F_P, see equations (2.9) and (2.21), has a pole of order $q-2$ at $P_{(a,b)}$ and no other poles. Since we already have seen that $H(P)$ has multiplicity $q-1$ or $q-2$, the conclusion is that the multiplicity is $q-2$. □

Remark 5.9. Let us denote by W_q the total number of Weierstrass points. We have seen that

$$\begin{aligned} W_q &= -(q+1)^2 + (q+1) + 2(q+1)m + (q+1)^2\left(\sum_{i=0}^{m-1}\varphi(i+1) - \sum_{i=0}^{(m-1)/p-1}\varphi(p\cdot(i+1))\right) \\ &= -(q+1)^2 + (q+1) + 2(q+1)m + (q+1)^2\left(\sum_{i=1}^{m}\varphi(i) - \sum_{i=1}^{(m-1)/p}\varphi(p\cdot i)\right). \end{aligned}$$

Here the notation $\sum_{i=0}^{\xi}$ for $\xi \in \mathbb{R}_{\geq 0}$ is shorthand for $\sum_{i=0}^{\lfloor\xi\rfloor}$.

Using iteratively that

$$\sum_{i=1}^{(m-1)/p}\varphi(p\cdot i) = (p-1)\sum_{i=1}^{(m-1)/p}\varphi(i) + \sum_{i=1}^{(m-1)/p^2}\varphi(p\cdot i),$$

one obtains that

$$\sum_{i=1}^{(m-1)/p}\varphi(p\cdot i) = \sum_{e=1}^{\lfloor\log_p(m-1)\rfloor}(p-1)\sum_{i=1}^{(m-1)/p^e}\varphi(i).$$

It is well known, see for example [14, Thm.330], that $\sum_{i=1}^{N}\varphi(i) = \frac{3}{\pi^2}N^2 + O(N\log(N))$ asymptotically as $N \to \infty$.

Hence, we see that

$$\begin{aligned}\sum_{i=1}^{(m-1)/p} \varphi(p\cdot i) &= \sum_{e=1}^{\lfloor \log_p(m-1)\rfloor} \frac{3(p-1)(m-1)^2}{\pi^2 p^{2e}} + O\left(\sum_{e=1}^{\lfloor \log_p(m-1)\rfloor} \frac{m-1}{p^e}\log_p\left(\frac{m-1}{p^e}\right)\right)\\ &= \frac{3(p-1)(m-1)^2}{\pi^2}\frac{1-p^2/p^{2\lfloor \log_p(m-1)\rfloor}}{p^2-1}\\ &\qquad + O\left(\int_0^{\log_p(m-1)} \frac{m-1}{p^e}\log_p\left(\frac{m-1}{p^e}\right)de\right)\\ &= \frac{3(m-1)^2}{\pi^2(p+1)} - \frac{3p^2}{\pi^2(p+1)}\left(\frac{m-1}{p^{\lfloor \log_p(m-1)\rfloor}}\right)^2 + O(q\log(q))\\ &= \frac{3(m-1)^2}{\pi^2(p+1)} + O(q\log(q)).\end{aligned}$$

Going back to the number of Weierstrass points, we see that

$$\begin{aligned}W_q &= (q+1)^2\left(\sum_{i=1}^{m-1}\varphi(i) - \sum_{i=1}^{(m-1)/p}\varphi(p\cdot i)\right) + O(q^2)\\ &= (q+1)^2\left(\frac{3(m-1)^2}{\pi^2} - \frac{3(m-1)^2}{\pi^2(p+1)}\right) + O(q^3\log(q))\\ &= \frac{3(m-1)^2(q+1)^2}{\pi^2}\frac{p}{p+1} + O(q^3\log(q))\\ &= \frac{q^4}{3\pi^2}\frac{p}{p+1} + O(q^3\log(q)).\end{aligned}$$

Since the number of rational points is $O(q^3)$, this shows that for large q, the number of non-rational Weierstrass points, vastly outnumbers the number of rational Weierstrass points.

6. The full automorphism group $\mathrm{Aut}(\mathcal{X}_3)$ of $\mathcal{X}_3$

It turns out that knowing the Weierstrass semigroup of all $\mathbb{F}_{q^2}$-rational points on $\mathcal{X}_3$, allows us to determine the full automorphism group $\mathrm{Aut}(\mathcal{X}_3)$ of $\mathcal{X}_3$. We devote this section to this. One approach might be to use a result from [19], giving the automorphism group of a function field that is a Kummer extension of the rational function field. However, even though $\mathbb{F}_{q^2}(\mathcal{X}_3)/\mathbb{F}_{q^2}(x)$ is a Kummer extension of degree $q+1$, the results from [19] do not apply, since there are insufficiently many totally ramified places.

As before $q \equiv 2 \pmod 3$ and we denote by p the characteristic of $\mathbb{F}_{q^2}$. As discussed in Section 2, the function field $\mathbb{F}_{q^2}(\mathcal{X}_3)$ can be seen as a subfield of the Hermitian function field $\mathbb{F}_{q^2}(\mathcal{H})$, and the function field extension $\mathbb{F}_{q^2}(\mathcal{H})/\mathbb{F}_{q^2}(\mathcal{X}_3)$ is an unramified Galois extension of degree 3 (see Remark 2.4), with Galois group generated by the automorphism τ, defined in equation (2.3). This observation is useful when constructing automorphisms of the curve $\mathcal{X}_3$ (equivalently, of the function field $\mathbb{F}_{q^2}(\mathcal{X}_3)$).

Indeed, a way to find automorphisms of $\mathbb{F}_{q^2}(\mathcal{X}_3)$ is to consider the normalizer $N(\langle\tau\rangle)$ of $\langle\tau\rangle$ in $\mathrm{Aut}(\mathcal{H}) \cong \mathrm{PGU}(3,q)$. Doing so, the group $N(\langle\tau\rangle)/\langle\tau\rangle$ is theoretically guaranteed to be a subgroup of the full automorphism group of the fixed field $\mathbb{F}_{q^2}(\mathcal{X}_3)$ of $\langle\tau\rangle$. The group $N(\langle\tau\rangle)$ in $\mathrm{PGU}(3,q)$ is a well-known maximal subgroup stabilizing a self-polar triangle, see [15, Theorem A.10]. It has order $6(q+1)^2/\gcd(3,q+1) = 2(q+1)^2$ and is isomorphic to the semidirect product of an abelian group of order $(q+1)^2/3$ containing τ and a symmetric group of order 6. This explains the structure of the automorphism group described in Lemma 2.6.

We now begin our study of the full automorphism group of $\mathcal{X}_3$. Recall that $\mathcal{O}_0 := \{P_0^1,\dots,P_0^m\}$, $\mathcal{O}_\infty := \{P_\infty^1,\dots,P_\infty^m\}$ and $\mathcal{O}_m = \{P_{(a,0)} \mid a^m+1=0\}$. Moreover $\mathcal{O} = \mathcal{O}_0 \cup \mathcal{O}_\infty \cup \mathcal{O}_m$ as in equation (2.5).

Lemma 6.1. *Let $\mathcal{O}$ be the set defined in equation* (2.5)*. Then $\mathcal{O}$ is an orbit of* $\mathrm{Aut}(\mathcal{X}_3)$*.*

Proof. Since $\mathcal{X}_3$ is $\mathbb{F}_{q^2}$-maximal, its full automorphism group $\mathrm{Aut}(\mathcal{X}_3)$ is defined over $\mathbb{F}_{q^2}$ and hence acts on the set $\mathcal{X}_3(\mathbb{F}_{q^2})$, see for example [2, Lemma 2.4]. Let $H(P_{(a,b)})$ and $H(P)$ be the Weierstrass semigroups at a point $P_{(a,b)} \in \mathcal{X}_3(\mathbb{F}_{q^2}) \setminus \mathcal{O}$ and at $P \in \mathcal{O}$, respectively. Since the semigroups $H(P_{(a,b)})$ and $H(P)$ are not the same (see Theorems 4.2, 4.4 and 4.5), $\mathrm{Aut}(\mathcal{X}_3)$ acts separately on $\mathcal{O}$ and $\mathcal{X}_3(\mathbb{F}_{q^2}) \setminus \mathcal{O}$. Moreover, since from Corollary 2.19 $\mathcal{O}$ is an orbit of $G \subseteq \mathrm{Aut}(\mathcal{X}_3)$, we deduce that $\mathcal{O}$ is also an orbit of the entire $\mathrm{Aut}(\mathcal{X}_3)$. □

We now use that $\mathcal{O}$ is an orbit, to start investigating the p-Sylow subgroup of $\mathrm{Aut}(\mathcal{X}_3)$.

Lemma 6.2. *Let $q \geq 11$. Let S_p denote a Sylow subgroup of $|\mathrm{Aut}(\mathcal{X}_3)|$. Then $|S_p| < q$.*

Proof. Since S_p acts on $\mathcal{O}$ by Lemma 6.1, we see that S_p has at least one fixed point $P \in \mathcal{O}$. Without loss of generality, we can assume $P = P_{(a,0)}$, for some a such that $a^m + 1 = 0$. Since $\mathcal{X}_3$ has p-rank zero, S_p acts with long orbits on $\mathcal{O} \setminus \{P_{(a,0)}\}$, see [15, Lemma 11.129]. This implies that $|S_p| \leq q$.

Now suppose that $|S_p| = q$. Then $\mathrm{Aut}(\mathcal{X}_3)$ acts 2-transitively on $\mathcal{O}$ and the stabilizer of two points is cyclic in this action, since it is of order relatively prime to p (see [15, Theorem 11.49]). Moreover, from [18, Theorem 1.1], $\mathrm{Aut}(\mathcal{X}_3)$ has a regular normal subgroup N, unless:

- $\mathrm{Aut}(\mathcal{X}_3)$ is isomorphic to either $\mathrm{PSL}(2,q)$, $\mathrm{PGL}(2,q)$, or
- $q = \bar{q}^3$ and $\mathrm{Aut}(\mathcal{X}_3)$ is isomorphic to $\mathrm{PSU}(3,\bar{q})$ or $\mathrm{PGU}(3,\bar{q})$, or
- $\mathrm{Aut}(\mathcal{X}_3)$ is isomorphic to the Suzuki group $Sz(\bar{q})$ where $q = \bar{q}^2$.

The first two possibilities can be excluded, since in that case $|\mathrm{Aut}(\mathcal{X}_3)|$ would not be divisible by $2(q+1)^2$. Further, if $\mathrm{Aut}(\mathcal{X}_3)$ was isomorphic to the Suzuki group $Sz(\bar{q})$, then the characteristic would be two and $q = \bar{q}^2$ would be an even power of two. However, this is impossible, since $q \equiv 2 \pmod 3$. This means that $\mathrm{Aut}(\mathcal{X}_3)$ has a regular normal subgroup N. Then, from [6, Theorem 1.7.6], we see that $|\mathcal{O}| = q+1 = \ell^h$ for some $h \in \mathbb{Z}_{>0}$ and some prime number ℓ. If q is odd, this cannot happen as $q+1$ is divisible by 6. If q is even, we would get $|\mathcal{O}| = q+1 = 2^n+1 = \ell^h$. If $h = 1$, this would mean that ℓ is a Fermat prime, which is only possible if n is a power of two. However, since n is odd, this would imply $n = 1$. This is impossible, since $q \geq 11$. If $h > 1$, then from Catalan's Conjecture (Mihailescu's theorem [21]), we see that the only possibility is that $\ell = 3$ and $n = 3$. This is again not possible, since we assumed that $q \geq 11$. Hence, we conclude that the only possibility is $|S_2| < q$. □

Next is a lemma that will allow us to identify certain automorphisms of $\mathcal{X}_3$.

Lemma 6.3. *Let $\alpha \in \mathrm{Aut}(\mathcal{X}_3)$ and suppose that $\alpha(x)$ is a cube, when seen as a function of the Hermitian function field $\overline{\mathbb{F}}_{q^2}(\mathcal{H})$. Then α can be lifted to an automorphism $\bar{\alpha}$ of $\mathcal{H}$.*

Proof. Since α is an automorphism of $\mathcal{X}_3$, we know that $\alpha(y)^{q+1} + \alpha(x)^{(q+1)/3} + \alpha(x)^{2(q+1)/3} = 0$. Let $\alpha(x) = w^3$, where $w = w(u,v) \in \overline{\mathbb{F}}_{q^2}(\mathcal{H})$, and define

$$\bar{\alpha}(u) = w \quad \text{and} \quad \bar{\alpha}(v) = \frac{\alpha(y)}{\bar{\alpha}(u)}.$$

Then

$$\bar{\alpha}(u)^{q+1} + \bar{\alpha}(v)^{q+1} + 1 = w^{q+1} + \frac{\alpha(y)^{q+1}}{w^{q+1}} + 1 = \frac{\alpha(x)^{2(q+1)/3} + \alpha(y)^{q+1} + \alpha(x)^{(q+1)/3}}{w^{q+1}} = 0.$$

This means that $\bar{\alpha}$ preserves the defining equation of the Hermitian function field, and defines an automorphism of $\mathcal{H}$. □

Note that since all automorphisms of $\mathcal{H}$ are defined over $\mathbb{F}_{q^2}$, the automorphism $\bar{\alpha}$ will also be defined over $\mathbb{F}_{q^2}$. Therefore, if $\alpha(x)$ is a cube in $\overline{\mathbb{F}}_{q^2}(\mathcal{H})$, it was necessarily already a cube in $\mathbb{F}_{q^2}(\mathcal{H})$.

6.1. The full automorphism group $\mathrm{Aut}(\mathcal{X}_3)$*, q odd*

We wish to use the information that $\mathcal{O}$ is an orbit of $\mathrm{Aut}(\mathcal{X}_3)$ to show that, for odd $q \geq 11$, $\mathrm{Aut}(\mathcal{X}_3)$ coincides with the subgroup G constructed in Lemma 2.6. If $q = 5$, the plane curve defined by the (affine) equation $X^5 + X = Y^3$, is birationally equivalent to $\mathcal{X}_3$. The corresponding isomorphism of function fields is described as $x = wX + (wX)^{-1}, y = Y/X$, where $w^2 = 2$. This curve is known to have an automorphism group that is isomorphic to a semidirect product of a cyclic group of order 3 with $\mathrm{PGL}(2,5)$, see [15, Theorem 12.11]. In particular $|\mathrm{Aut}(\mathcal{X}_3)| = 360$ if $q = 5$, which is five times the cardinality of the group of automorphisms G described in Lemma 2.6.

From now, we assume in this subsection that $q \geq 11$ and q is odd. It turns out that in this case, the automorphism group of $\mathcal{X}_3$ actually coincides with G. To see why, let us first prove under the aforementioned hypotheses on q that $\mathrm{Aut}(\mathcal{X}_3)$ is tame, that is, it does not contain any element of order p.

Lemma 6.4. *Let $q \geq 11$ and q odd. Then $|\mathrm{Aut}(\mathcal{X}_3)|$ is not divisible by the characteristic p of the field $\mathbb{F}_{q^2}$.*

Proof. Suppose by contradiction that $\mathrm{Aut}(\mathcal{X}_3)$ admits a Sylow p-subgroup S_p of order p^i for some $i \geq 1$. As we have seen in the proof of Lemma 6.2, we may assume that S_p fixes $P \in \mathcal{O}$, where $P = P_{(a,0)}$, for some a such that $a^m + 1 = 0$ and that S_p acts with long orbits on $\mathcal{O} \setminus \{P_{(a,0)}\}$. Further by Lemma 6.2, we may assume that $|S_p| < q$.

Recall that the automorphism $\sigma : (x, y) \mapsto (x, \delta y)$, where δ is a primitive $(q+1)$-th root of unity, fixes the set $\mathcal{O}_m$ point-wise, while it acts transitively on the sets $\mathcal{O}_0$ and $\mathcal{O}_\infty$. From this, it follows that σ normalizes S_p (see [15, Theorem 11.49]) and preserves the orbit of S_p containing $\mathcal{O}_m$. We have thus two possibilities for a fixed $\bar{a}$: either the orbit of S_p containing $P_{(\bar{a},0)}$ is contained in $\mathcal{O}_m$, or it contains entirely either $\mathcal{O}_0$ or $\mathcal{O}_\infty$. In the second case, we would get that $|S_p| \geq (q+1)/3 + 1$ and hence $|S_p| = q$, which is not possible. Therefore, we can deduce that, for all $\bar{a}$ with $\bar{a}^m + 1 = 0$, the S_p-orbit of $P_{(\bar{a},0)}$ is contained in $\mathcal{O}_m$. Since S_p acts on $\mathcal{O} = \mathcal{O}_m \cup \mathcal{O}_0 \cup \mathcal{O}_\infty$, S_p must then act with long orbits on $\mathcal{O}_0 \cup \mathcal{O}_\infty$, which is a set of cardinality $2(q+1)/3$. We hence obtain the desired contradiction, as $2(q+1)/3$ is not divisible by p. □

Theorem 6.5. *Let $q \geq 11$, q odd. Then $\mathrm{Aut}(\mathcal{X}_3) = G$.*

Proof. Suppose by contradiction that $|\mathrm{Aut}(\mathcal{X}_3)| > |G|$. Let $G_{P_{(a,0)}}$ be the stabilizer in G of $P_{(a,0)}$, for an a such that $a^m + 1 = 0$. Since, by the orbit-stabilizer theorem, $|G| = |\mathcal{O}||G_{P_{(a,0)}}|$ and, by Lemma 6.1, $\mathcal{O}$ is an orbit of $\mathrm{Aut}(\mathcal{X}_3)$, the stabilizer $\mathrm{Aut}(\mathcal{X}_3)_{P_{(a,0)}}$ of $P_{(a,0)}$ in $\mathrm{Aut}(\mathcal{X}_3)$ contains some extra automorphism $\gamma \notin G_{P_{(a,0)}}$. Let C_{q+1} be the cyclic group generated by $\sigma : (x, y) \mapsto (x, \delta y)$, where δ is a primitive $(q+1)$-th root of unity. Then, since $\mathrm{Aut}(\mathcal{X}_3)_{P_{(a,0)}}$ is cyclic (as follows from the fact that $\mathrm{Aut}(\mathcal{X}_3)$ is of order relatively prime to p), γ commutes with C_{q+1} and hence it acts on its fixed points (and, in general, orbits). This means that γ acts on the sets $\mathcal{O}_m$ and $\mathcal{O}_0 \cup \mathcal{O}_\infty$, because the set $\mathcal{O}_m$ is exactly the set of fixed points of C_{q+1}. Since $\mathcal{O}_0$ and $\mathcal{O}_\infty$ are orbits of C_{q+1} of the same length, either γ fixes both $\mathcal{O}_0$ and $\mathcal{O}_\infty$, or interchanges them.

If γ fixes both $\mathcal{O}_0$ and $\mathcal{O}_\infty$, then it fixes the divisor of x from equation (2.17). This means that $\gamma(x) = \lambda x$, for some constant λ. Hence, $\gamma(x)$ is a cube in $\overline{\mathbb{F}}_{q^2}(\mathcal{H})$, as $x = u^3$ and λ is a constant. Suppose instead that γ interchanges $\mathcal{O}_0$ and $\mathcal{O}_\infty$. Then, γ maps the divisor of x to the divisor of $\frac{1}{x}$, meaning that there exists a constant λ such that $\gamma(x) = \frac{\lambda}{x}$. Hence, in all cases $\alpha(x)$ is a cube in $\overline{\mathbb{F}}_{q^2}(\mathcal{H})$.

From Lemma 6.3, γ can be lifted to an automorphism $\bar{\gamma}$ of the Hermitian curve $\mathcal{H}$ acting on the set of $3(q+1)$ points above those in $\mathcal{O}$. Those points are geometrically the intersection of the Hermitian curve $\mathcal{H}$ with 3 lines intersecting each other in 3 points outside $\mathcal{H}$, that is a self-polar triangle. Since this shows that γ is induced by $N(\langle\sigma\rangle)$, then $\gamma \in G$, which gives a contradiction. □

6.2. The full automorphism group $\mathrm{Aut}(\mathcal{X}_3)$*, q even*

We now turn our attention to the case where q is even, that is to say when $q = 2^n$, n odd. If $q = 2$, the curve is isomorphic to the Hermitian curve over $\mathbb{F}_4$ and therefore has $\mathrm{PGU}(3, 2)$ as automorphism group, which contains 216 elements. Here only automorphisms defined over $\mathbb{F}_{q^2}$ were considered. Hence in this case, there are twelve times more automorphisms than described in Lemma 2.6. If $q = 8$, the automorphism group of $\mathcal{X}_3$ is known, as in this case $\mathcal{X}_3$ is isomorphic to the Giulietti-Korchmáros maximal curve (see [12]). This curve can for example be given as a plane curve with affine equation $Y^9 = (X^2 + X)(X^2 + X + 1)^3$. An explicit isomorphism on the level of function fields is then given by $X = \zeta_3 + (x^5 + x^4 + x^3)/y^9$ and $Y = (x^5 + x^4 + x^3)/y^8$. Hence for $q = 8$, the automorphism group of X_3 is a semidirect product of a cyclic group of order 3 and $\mathrm{PGU}(3, 2)$, resulting in 648 automorphisms, four times more than the group from Lemma 2.6 contains.

From the remainder of this subsection, we will assume that $q = 2^n$, n odd and at least five. We will now show that in this case the automorphism group of $\mathcal{X}_3$ coincides with the group G from Lemma 2.6. To this aim, a similar argument as in the previous subsection will be provided. Of course in this case we cannot prove that $\mathrm{Aut}(\mathcal{X}_3)$ is tame, as G itself is non-tame. We will in fact first prove that, if a Sylow 2-subgroup of $\mathrm{Aut}(\mathcal{X}_3)$ has order larger than 2, then its cardinality must be $q/2$.

Lemma 6.6. *Let $n \geq 5$ and $q = 2^n$. Let also S_2 denote a Sylow 2-subgroup of $\mathrm{Aut}(\mathcal{X}_3)$. Then either $|S_2| = 2$ or $|S_2| = q/2$. In the latter case, a 2-Sylow S_2 fixing a point $P_{(a,0)}$, with $a^m + 1 = 0$, acts on $\mathcal{O}$ with the following 3 orbits:*

- $\{P_{(a,0)}\}$,
- $\mathcal{O}_1^{S_2} := \mathcal{O}_0 \cup \{P_{(\beta_1,0)}, \ldots, P_{(\beta_{(q-2)/6},0)}\}$,
- $\mathcal{O}_2^{S_2} := \mathcal{O}_\infty \cup \{P_{(\gamma_1,0)}, \ldots, P_{(\gamma_{(q-2)/6},0)}\}$,

where $\{P_{(a,0)}\}$, $\{P_{(\beta_1,0)}, \ldots, P_{(\beta_{(q-2)/6,0})}\}$ and $\{P_{(\gamma_1,0)}, \ldots, P_{(\gamma_{(q-2)/6,0})}\}$ is a suitably chose partition of $\mathcal{O}_m$.

Proof. Let S_2 be of order 2^i for some $i \geq 1$. Just as in the proof of Lemma 6.4, we may assume that S_2 fixes $P \in \mathcal{O}$, where $P = P_{(a,0)}$, for some a such that $a^m + 1 = 0$ and that S_2 acts with long orbits on $\mathcal{O} \setminus \{P_{(a,0)}\}$. Further by Lemma 6.2, we may assume that $|S_2| < q$.

Recall that the automorphism $\sigma : (x, y) \mapsto (x, \delta y)$, where δ is a primitive $(q + 1)$-th root of unity, fixes $P_{(a,0)}$ and hence normalizes S_2, from [15, Theorem 11.49]. Moreover, σ fixes the set $\mathcal{O}_m$ point-wise, while it acts transitively on $\mathcal{O}_0$ and $\mathcal{O}_\infty$. This means that σ preserves the orbit of S_2 containing $P_{(\bar{a},0)}$, for $\bar{a}$ such that $\bar{a}^m + 1 = 0$. We have thus two possibilities for a fixed $\bar{a}$: either the orbit of S_2 containing $P_{(\bar{a},0)}$ is contained in $\mathcal{O}_m$, or it contains entirely either $\mathcal{O}_0$ or $\mathcal{O}_\infty$.

If the second case never occurs, then S_2 acts semiregularly on $\mathcal{O}_0 \cup \mathcal{O}_\infty$, which is a set of cardinality $2(q + 1)/3$. This implies that $|S_2| = 2$. If the second case occurs for some a, then we get that $|S_2| \geq (q + 1)/3 + 1$ and hence $|S_2| = q/2$. Note that in this case the only possible configuration of orbits of S_2 acting on the q points in $\mathcal{O}_m \setminus \{P_{(a,0)}\}$ is that S_2 has exactly 2 orbits of length $q/2$: one $\mathcal{O}_1^{S_2}$ containing $\mathcal{O}_0$ and $(q-2)/6$ points of $\mathcal{O}_m$, and another one $\mathcal{O}_2^{S_2}$ containing $\mathcal{O}_\infty$ and the remaining $(q - 2)/6$ points in $\mathcal{O}_m$. □

We now exclude the second case in Lemma 6.6.

Lemma 6.7. *The case $|S_2| = q/2$ cannot occur.*

Proof. Suppose by contradiction $|S_2| = q/2$. With notation as in Lemma 6.6, we can assume that S_2 acts on $\mathcal{O}$ with three orbits $\{P_{(a,0)}\}$, $\mathcal{O}_1^{S_2}$ and $\mathcal{O}_2^{S_2}$. The cyclic group C_{q+1}, generated by $\sigma : (x, y) \mapsto (x, \delta y)$, where δ is a primitive $(q + 1)$-th root of unity, fixes any point in $\mathcal{O}_m$, in particular $P_{(a,0)}$, and hence normalizes S_2. In particular, the group L generated by σ and the elements of S_2 has $|S_2|(q + 1)$ many elements. Since the stabilizer of two points is tame and cyclic, we conclude that C_{q+1} is the two points stabilizer of the points $P_{(a,0)}$ and any other $P \in \mathcal{O}_m$.

Using the notation from Lemma 6.6, choose $\gamma \in S_2$ be such that $\gamma(P_{(\beta_1,0)}) = P_{(\beta_2,0)}$, with $P_{(\beta_1,0)}, P_{(\beta_2,0)} \in \mathcal{O}_1^{S_2}$ distinct. Such a γ exists, since $P_{(\beta_1,0)}$ and $P_{(\beta_2,0)}$ are in the same orbit under the action of S_2. Then $\gamma^{-1} \cdot \sigma \cdot \gamma$ fixes $P_{(a,0)}$ and $\gamma^{-1} \cdot \sigma \cdot \gamma(P_{(\beta_1,0)}) = \gamma^{-1} \cdot \sigma(P_{(\beta_2,0)}) = \gamma^{-1}(P_{(\beta_2,0)}) = P_{(\beta_1,0)}$. Hence, $\gamma^{-1} \cdot \sigma \cdot \gamma$ is an element of order $q+1$ fixing both $P_{(a,0)}$ and $P_{(\beta_1,0)}$. Hence $\gamma^{-1} \cdot \sigma \cdot \gamma \in C_{q+1}$ and more specifically $\gamma^{-1} \cdot \sigma \cdot \gamma = \sigma^k$, where $(k, q + 1) = 1$. Moreover, since C_{q+1} normalizes S_2, there exists $\tilde{\gamma} \in S_2$ such that $\sigma \cdot \gamma = \tilde{\gamma} \cdot \sigma$. Hence $\mathrm{id} = \gamma^{-1} \cdot \sigma \cdot \gamma \cdot \sigma^{-k} = \gamma^{-1}\tilde{\gamma} \cdot \sigma^{1-k}$. Since $S_2 \cap C_{q+1} = \{\mathrm{id}\}$, this implies that $k = 1$ and hence that γ and σ commute.

Now let ι be a suitable power of γ such that ι has order two. Then for any $P_{(\beta_j,0)} \in \mathcal{O}_1^{S_2}$, we have $\iota(P_{(\beta_j,0)}) \in \mathcal{O}_1^{S_2}$, since S_2 acts on $\mathcal{O}_1^{S_2}$. On the other hand, using that σ and ι commute and that σ fixes all points in $\mathcal{O}_m$, we have $\sigma \cdot \iota(P_{(\beta_j,0)}) = \iota \cdot \sigma(P_{(\beta_j,0)}) = \iota(P_{(\beta_j,0)})$. Hence $\iota(P_{(\beta_j,0)})$ is a fixed point of σ, which implies that $\iota(P_{(\beta_j,0)}) \in \mathcal{O}_m$. We conclude that $\iota(P_{(\beta_j,0)}) \in \mathcal{O}_1^{S_2} \cap \mathcal{O}_m = \{P_{(\beta_1,0)}, \ldots, P_{(\beta_{(q-2)/6},0)}\}$. In other words: ι acts on $\{P_{(\beta_1,0)}, \ldots, P_{(\beta_{(q-2)/6},0)}\}$. Since $(q - 2)/6 = (q/2 + 1)/3$ is an odd number, this implies that ι has, apart from $P_{(a,0)}$, at least one more fixed point. However, since the characteristic is two, this is impossible according to [15, Lemma 11.129]. □

We are now ready to compute $\mathrm{Aut}(\mathcal{X}_3)$ when q is even.

Theorem 6.8. *Let* $q = 2^n$, $n \geq 5$ *odd. Then* $\mathrm{Aut}(\mathcal{X}_3) = G$.

Proof. Combining Lemmas 6.6 and 6.7, we conclude that $|S_2| = 2$. Suppose by contradiction that $|\mathrm{Aut}(\mathcal{X}_3)| > |G|$. Let $G_{P_{(a,0)}}$ be the stabilizer in G of $P_{(a,0)}$, for a such that $a^m + 1 = 0$. Since, by the orbit-stabilizer theorem, $|G| = |\mathcal{O}||G_{P_{(a,0)}}|$ and, by Lemma 6.1, $\mathcal{O}$ is an orbit of $\mathrm{Aut}(\mathcal{X}_3)$, the stabilizer $\mathrm{Aut}(\mathcal{X}_3)_{P_{(a,0)}}$ of $P_{(a,0)}$ in $\mathrm{Aut}(\mathcal{X}_3)$ contains some extra automorphism $\gamma \notin G_{P_{(a,0)}}$. Also, since $|S_2| = 2$ and $|G| = 2(q+1)^2$, γ can be assumed to be of odd order.

Let C_{q+1} be the cyclic group generated by $\sigma : (x, y) \mapsto (x, \delta y)$, where δ is a primitive $(q+1)$-th root of unity. Then, since the tame part of $\mathrm{Aut}(\mathcal{X}_3)_{P_{(a,0)}}$ is cyclic, γ commutes with C_{q+1} and hence it acts on its fixed points (and, in general, orbits). At this point, the remainder of the proof is exactly the same as the proof of Theorem 6.5. □

Data availability

No data was used for the research described in the article.

References

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

[2] D. Bartoli, M. Montanucci, F. Torres, $\mathbb{F}_{p^2}$-maximal curves with many automorphisms are Galois-covered by the Hermitian curve, Adv. Geom. 21 (2021) 325–336.

[3] D. Bartoli, M. Montanucci, G. Zini, Weierstrass semigroups at every point of the Suzuki curve, Acta Arith. 197 (2021) 1–20.

[4] P. Beelen, L. Landi, M. Montanucci, Weierstrass semigroups on the Skabelund maximal curve, Finite Fields Appl. 72 (2021) 101811.

[5] P. Beelen, M. Montanucci, Weierstrass semigroups on the Giulietti–Korchmáros curve, Finite Fields Appl. 52 (2018) 10–29.

[6] N.L. Biggs, A.T. White, Permutation Groups and Combinatorial Structures, London Mathematical Society Lecture Note Series, vol. 33, Cambridge University Press, Cambridge-New York, 1979.

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

[8] R. Fuhrmann, F. Torres, The genus of curves over finite fields with many rational points, Manuscr. Math. 89 (1996) 103–106.

[9] R. Fuhrmann, F. Torres, On Weierstrass points and optimal curves, Rend. Circ. Mat. Palermo Suppl. 51 (1998) 25–46.

[10] A. Garcia, F. Torres, On maximal curves having classical Weierstrass gaps, in: Applications of Curves over Finite Fields, Seattle, WA, 1997, in: Contemp. Math., vol. 245, Amer. Math. Soc., Providence, RI, 1999, pp. 49–59.

[11] A. Garcia, P. Viana, Weierstrass points on certain non-classical curves, Arch. Math. 46 (1986) 315–322.

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

[13] V.D. Goppa, Geometry and Codes, Math. Appl. Kluwer, Dordrecht, 1988.

[14] G.H. Hardy, E.M. Wright, An Introduction to the Theory of Numbers, 3rd ed., Oxford, at the Clarendon Press, 1960.

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

[16] T. Høholdt, J.H. van Lint, R. Pellikaan, Algebraic geometry codes, in: V.S. Pless, W.C. Huffman, R.A. Brualdi (Eds.), Handbook of Coding Theory, vol. 1, Elsevier, Amsterdam, The Netherlands, 1998, pp. 871–961.

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

[18] W.M. Kantor, M.E. O'Nan, G.M. Seitz, 2-transitive groups in which the stabilizer of two points is cyclic, J. Algebra 21 (1972) 17–50.

[19] A. Kontogeorgis, The group of automorphisms of cyclic extensions of rational function fields, J. Algebra 216 (1999) 665–706.

[20] G. Korchmáros, F. Torres, On the genus of a maximal curve, Math. Ann. 323 (2002) 589–608.

[21] P. Mihailescu, Primary cyclotomic units and a proof of Catalan's conjecture, J. Reine Angew. Math. 572 (2004) 167–195.

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

[23] H. Stichtenoth, Algebraic Function Fields and Codes, second edition, Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009.

[24] K.O. Stöhr, J.F. Voloch, Weierstrass points and curves over finite fields, Proc. Lond. Math. Soc. 52 (1986) 1–19.

[25] S. Tafazolian, F. Torres, On the Ree curve, J. Pure Appl. Algebra 223 (2019) 3831–3842.

[26] M.A. Tsfasman, S. Vladut, Algebraic-Geometric Codes, Kluwer, Dordrecht, 1991.

[27] G.D. Villa Salvador, Topics in the Theory of Algebraic Function Fields, Mathematics: Theory and Applications, Birkhäuser Boston, Inc., Boston, MA, 2006.