Weierstrass semigroups on the Giulietti–Korchmáros curve

Beelen, Peter ; Montanucci, Maria

Published in:
Finite Fields and Their Applications

Link to article, DOI:
10.1016/j.ffa.2018.03.002

Publication date:
2018

Document Version
Peer reviewed version

Weierstrass semigroups on the Giulietti–Korchmáros curve

Peter Beelen and Maria Montanucci

Abstract

In this article we explicitly determine the structure of the Weierstrass semigroups $H(P)$ for any point P of the Giulietti–Korchmáros curve $\mathcal{X}$. We show that as the point varies, exactly three possibilities arise: One for the $\mathbb{F}_{q^2}$-rational points (already known in the literature), one for the $\mathbb{F}_{q^6} \setminus \mathbb{F}_{q^2}$-rational points, and one for all remaining points. As a result, we prove a conjecture concerning the structure of $H(P)$ in case P is a $\mathbb{F}_{q^6} \setminus \mathbb{F}_{q^2}$-rational point. As a corollary we also obtain that the set of Weierstrass points of $\mathcal{X}$ is exactly its set of $\mathbb{F}_{q^6}$-rational points.

Math. Subj. Class.: Primary: 11G20. Secondary: 11R58, 14H05, 14H55.
Keywords: Giulietti–Korchmáros maximal curve, Weierstrass semigroup, Weierstrass points.

1 Introduction

Let $\mathcal{C}$ be a nonsingular, projective algebraic curve of genus g defined over a field $\mathbb{F}$. Let P be a rational point on $\mathcal{C}$. The *Weierstrass semigroup* $H(P)$ is defined as the set of integers k such that there exists a function on $\mathcal{C}$ having pole divisor exactly kP. More generally $H(P)$ can be defined for any point P on $\mathcal{C}$ by considering $\mathcal{C}$ as an algebraic curve over the algebraic closure of $\mathbb{F}$. It is clear that $H(P)$ is a subset of natural numbers $\mathbb{N} = \{0, 1, 2, \ldots\}$. The Weierstrass gap Theorem, see [10, Theorem 1.6.8], states that the set $G(P) := \mathbb{N} \setminus H(P)$ contains exactly g elements, which are called *gaps*. The structure of $H(P)$ is not always the same for every point P of $\mathcal{C}$. However, it is known that for generically the semigroup $H(P)$ is the same, but there can exist finitely many points of $\mathcal{C}$, called *Weierstrass points*, with a different gap set. These points are of intrinsic interest, for example in Stöhr–Voloch theory [11], but in case $\mathbb{F} = \mathbb{F}_q$, the finite field with q elements, they also occur in the study of algebraic geometry (AG) codes [12]. In this context, a commonly studied class of curves are the so-called *maximal curves*, that is, algebraic curves defined over a finite field $\mathbb{F}_q$ having as many rational points as possible according to the Hasse–Weil bound. More precisely, an algebraic curve $\mathcal{C}$ with genus $g(\mathcal{C})$ and defined over $\mathbb{F}_q$ is said to be an $\mathbb{F}_q$-maximal curve if it has $q + 1 + 2g(\mathcal{C})\sqrt{q}$ points defined over $\mathbb{F}_q$. Clearly, this can only be the case if the cardinality q of the finite field is a square.

An important and well-studied example of an $\mathbb{F}_{q^2}$-maximal curve is given by the Hermitian curve $\mathcal{H}$. For fixed q, the curve $\mathcal{H}$ has the largest possible genus $g(\mathcal{H}) = q(q-1)/2$ that an $\mathbb{F}_{q^2}$-maximal curve can have. The Weierstrass points on $\mathcal{H}$ and the precise structure of the semigroups for P on $\mathcal{H}$ are known; see [3]. By a result commonly attributed to Serre, see [9, Proposition 6], any $\mathbb{F}_{q^2}$-rational curve which is covered by an $\mathbb{F}_{q^2}$-maximal curve is also $\mathbb{F}_{q^2}$-maximal. Most of the known maximal curves are subcovers of the Hermitian curve. The first known example of a maximal curve which is not a subcover of the Hermitian curve was constructed by Giulietti and Korchmáros; see [4]. This curve is an $\mathbb{F}_{q^6}$-maximal curve and commonly called the Giulietti–Korchmáros (GK) curve. The aim of this paper is to complete the description of the Weierstrass semigroups occurring for this curve.

The Weierstrass semigroup for any $\mathbb{F}_{q^2}$-rational point of $\mathcal{X}$ was computed in [4], but the structure of the Weierstrass semigroup $H(P)$ where $P \notin \mathcal{X}(\mathbb{F}_{q^2})$ is not known, except for $q \leq 9$, [2, 1]. Based on the available data for small q, a conjecture concerning the structure of $H(P)$ was stated in [1] for $P \in \mathcal{X}(\mathbb{F}_{q^6}) \setminus \mathcal{X}(\mathbb{F}_{q^2})$. For $P \notin \mathcal{X}(\mathbb{F}_{q^6})$ nothing specific is known about $H(P)$. In this article we determine settle the conjecture from [1] and also determine the structure of the generic semigroup for P on $\mathcal{X}$. More precisely, we show the following theorem.

Theorem 1.1. *Let q be a prime power and let P be a point of the Giulietti–Korchmáros curve $\mathcal{X}$. The Weierstrass semigroup $H(P)$ is given by*

- $H(P) = \langle q^3 - q^2 + q, q^3, q^3 + 1 \rangle$, *if $P \in \mathcal{X}(\mathbb{F}_{q^2})$;*
- $H(P) = \langle q^3 - q + 1, q^3 + 1, q^3 + i(q^4 - q^3 - q^2 + q - 1) \mid i = 0, \ldots, q-1 \rangle$, *if $P \in \mathcal{X}(\mathbb{F}_{q^6}) \setminus \mathcal{X}(\mathbb{F}_{q^2})$;*
- $H(P) = \mathbb{N} \setminus G$, *if $P \notin \mathcal{X}(\mathbb{F}_{q^6})$, where*

$$G = \left\{ iq^3 + kq + m(q^2+1) + \sum_{s=1}^{q-2} n_s((s+1)q^2) + j + 1 \mid i, j, k, m, n_1, \ldots, n_{q-2} \in \mathbb{Z}_{\geq 0},\ j \leq q-1 \text{ and } \right.$$
$$\left. i + j + k + mq + \sum_{s=1}^{q-2} n_s((s+1)q - s) \leq q^2 - 2 \right\}.$$

As mentioned above, the case $P \in \mathcal{X}(\mathbb{F}_{q^2})$ is already known and taken from [4]. As a bonus, we will also obtain the set of Weierstrass points of $\mathcal{X}$.

Corollary 1.2. *Let W denote the set of Weierstrass points of the Giulietti–Korchmáros curve $\mathcal{X}$. Then $W = \mathcal{X}(\mathbb{F}_{q^6})$.*

The paper is organized as follows: In the next section we give the necessary background on the GK curve as well as some results on Weierstrass semigroups and their gaps that we will need later. In section three, we settle the conjecture from [1] concerning $H(P)$ for $P \in \mathcal{X}(\mathbb{F}_{q^6}) \setminus \mathcal{X}(\mathbb{F}_{q^2})$, while in section four, we compute the Weierstrass semigroup for $P \notin \mathcal{X}(\mathbb{F}_{q^6})$. We finish with some concluding remarks and observations.

2 The Giulietti–Korchmáros curve

Let q be a prime power and $\mathbb{K} = \overline{\mathbb{F}}_q$. The Giulietti–Korchmáros (GK) curve $\mathcal{X}$ is a non-singular curve in $\mathrm{PG}(3, \mathbb{K})$ defined by the affine equations

$$\mathcal{X} : \begin{cases} Y^{q+1} = X^q + X, \\ Z^{q^2-q+1} = Y^{q^2} - Y. \end{cases} \tag{1}$$

This curve has genus $g(\mathcal{X}) = (q^5 - 2q^3 + q^2)/2$ and $q^8 - q^6 + q^5 + 1$ $\mathbb{F}_{q^6}$-rational points. The curve $\mathcal{X}$ has been introduced in [4], where it was proved that $\mathcal{X}$ is maximal over $\mathbb{F}_{q^6}$, that is, the number $|\mathcal{X}(\mathbb{F}_{q^6})|$ of $\mathbb{F}_{q^6}$-rational points of $\mathcal{X}$ equals $q^6 + 1 + 2gq^3$. Also, for $q > 2$, the curve $\mathcal{X}$ is not $\mathbb{F}_{q^6}$-covered by the Hermitian curve maximal over $\mathbb{F}_{q^6}$; $\mathcal{X}$ was the first maximal curve shown to have this property. Note that equation (1) implies that $\mathcal{X}$ is a cover of the Hermitian curve over $\mathbb{F}_{q^2}$ given by the affine equation $Y^{q+1} = X^q + X$. We will denote this curve by $\mathcal{H}$.

The automorphism group $\mathrm{Aut}(\mathcal{X})$ of $\mathcal{X}$ is defined over $\mathbb{F}_{q^6}$ and has order $q^3(q^3+1)(q^2-1)(q^2-q+1)$. Moreover, it has a normal subgroup isomorphic to $\mathrm{SU}(3,\mathrm{q})$, the automorphism group of the Hermitian curve $\mathcal{H}$. The set $\mathcal{X}(\mathbb{F}_{q^6})$ of the $\mathbb{F}_{q^6}$-rational points of $\mathcal{X}$ splits into two orbits under the action of $\mathrm{Aut}(\mathcal{X})$: one orbit $\mathcal{O}_1 = \mathcal{X}(\mathbb{F}_{q^2})$ of size q^3+1, which coincides with the intersection between $\mathcal{X}$ and the plane $Z=0$; and another orbit $\mathcal{O}_2 = \mathcal{X}(\mathbb{F}_{q^6}) \setminus \mathcal{X}(\mathbb{F}_{q^2})$ of size $q^3(q^3+1)(q^2-1)$; see [4, Theorem 7]. The orbits $\mathcal{O}_1$ and $\mathcal{O}_2$ are the short orbits of $\mathrm{Aut}(\mathcal{X})$, that is, the unique orbits of points of $\mathcal{X}$ having a non-trivial stabilizer in $\mathrm{Aut}(\mathcal{X})$.

Let $x, y, z \in \mathbb{K}(\mathcal{X})$ be the coordinate functions of the function field of $\mathcal{X}$, which satisfy $y^{q+1} = x^q + x$ and $z^{q^2-q+1} = y^{q^2} - y$. Then we denote by $P_{(a,b,c)}$ the affine point of $\mathcal{X}$ with coordinates (a,b,c) and by P_∞ the unique point at infinity. Similarly, we denote by $Q_{(a,b)}$ the affine point of the Hermitian curve $\mathcal{H}$ with coordinates (a,b) and by Q_∞ its unique point at infinity.

The Weierstrass semigroup at P_∞, and hence at every $\mathbb{F}_{q^2}$-rational point of $\mathcal{X}$ (since they lie in the same short orbit $\mathcal{O}_1$ of $\mathrm{Aut}(\mathcal{X})$) was computed in [4].

Proposition 2.1. [4, Proposition 6.2] The Weierstrass semigroup of $\mathcal{X}$ at P_∞ is generated by q^3-q^2+q, q^3, q^3+1.

Before describing what is known about $H(P)$ for $P \notin \mathcal{X}(\mathbb{F}_{q^2})$, we introduce several functions on $\mathcal{X}$ and give their divisors. Some of these functions can be interpreted as functions on $\mathcal{H}$ as well and therefore have a divisor on $\mathcal{H}$. To differentiate, we will write $(f)_{\mathcal{H}}$ (resp. $(f)_{\mathcal{X}}$) for divisors on the Hermitian curve $\mathcal{H}$ (resp. the GK curve $\mathcal{X}$). Given a point $P = P_{(a,b,c)}$ on $\mathcal{X}$, we define the functions

$$\tilde{x}_P = -a^q - x + b^q y, \quad \tilde{y}_P = y - b, \quad \tilde{z}_P = -a^{q^3} - x + b^{q^3} y + c^{q^3} z. \tag{2}$$

Then it is not hard to show the following.

$$(\tilde{x}_P)_{\mathcal{X}} = q \sum_{\xi^{q^2-q+1}=1} P_{(a,b,\xi c)} + \sum_{\xi^{q^2-q+1}=1} P_{(a^{q^2}, b^{q^2}, \xi c^{q^2})} - (q^3+1)P_\infty, \tag{3}$$

$$(\tilde{y}_P)_{\mathcal{X}} = \sum_{s^q+s=0,\ \xi^{q^2-q+1}=1} P_{(a+s,b,\xi c)} - (q^3-q^2+q)P_\infty, \tag{4}$$

$$(\tilde{z}_P)_{\mathcal{X}} = q^3 P_{(a,b,c)} + P_{(a^{q^6}, b^{q^6}, c^{q^6})} - (q^3+1)P_\infty, \tag{5}$$

$$(z)_{\mathcal{X}} = \sum_{P \in \mathcal{X}(\mathbb{F}_{q^2}), P \neq P_\infty} P \; - \; q^3 P_\infty. \tag{6}$$

Now let $P = P_{(a,b,c)}$ be a fixed $\mathbb{F}_{q^6}$-rational point of $\mathcal{X}$ which is not $\mathbb{F}_{q^2}$-rational (implying $c \neq 0$). In this case equation (5) implies:

$$(\tilde{z}_P)_{\mathcal{X}} = (q^3+1)(P - P_\infty) \text{ for } P = P_{(a,b,c)} \in \mathcal{X}(\mathbb{F}_{q^6}). \tag{7}$$

The Weierstrass semigroup $H(P)$ is only completely known in finitely many cases if $P \in \mathcal{X}(\mathbb{F}_{q^6}) \setminus \mathcal{X}(\mathbb{F}_{q^2})$. It was computed for $q=2$ and $q=3$ in [2] and for $4 \leq q \leq 9$ in [1]. Also in [1], the following partial information was obtained for general q: Equations (3), (4) and (7) imply that the functions $1/\tilde{z}_P, \tilde{y}_P/\tilde{z}_P, \tilde{x}_P/\tilde{z}_P$ have poles only in P of orders q^3+1, q^3 and q^3-q+1 respectively. Hence

$$\langle q^3-q+1, q^3, q^3+1 \rangle \subseteq H(P) \text{ for } P \in \mathcal{X}(\mathbb{F}_{q^6}) \setminus \mathcal{X}(\mathbb{F}_{q^2}). \tag{8}$$

Based on this and the results for $q \leq 9$, the following conjecture was stated in [1], which we will prove in the next section.

Conjecture 2.2. *The Weierstrass semigroup $H(P)$ of $\mathcal{X}$ at $P \in \mathcal{X}(\mathbb{F}_{q^6}) \setminus \mathcal{X}(\mathbb{F}_{q^2})$ is given by*

$$H(P) = \langle q^3 - q + 1, q^3 + 1, q^3 + i(q^4 - q^3 - q^2 + q - 1) \mid i = 0, \ldots, q-1 \rangle.$$

Finally, for $P \notin \mathcal{X}(\mathbb{F}_{q^6})$ nothing specific is known about the structure of semigroup $H(P)$. We will completely determine its gap structure, but for now, we finish this section by stating some facts that we will use to achieve this. We start with the following well-known lemma connecting regular differentials (i.e., differential forms having no poles anywhere on $\mathcal{X}$) and gaps of $H(P)$.

Proposition 2.3. [13, Corollary 14.2.5] *Let $\mathcal{X}$ be an algebraic curve of genus g defined over $\mathbb{K}$. Let P be a point of $\mathcal{X}$ and ω be a regular differential on $\mathcal{X}$. Then $v_P(\omega) + 1$ is a gap at P.*

This proposition has the following, for us very useful, consequence.

Corollary 2.4. *For any point P on the GK curve $\mathcal{X}$ distinct from P_∞ and for any $f \in L((2g(\mathcal{X}) - 2)P_\infty)$, we have $v_P(f) + 1 \in \mathbb{N} \backslash H(P)$.*

Proof. First note that $(dy)_{\mathcal{H}} = (q^2 - q - 2)Q_\infty$. The set of points that ramify in the covering of $\mathcal{X}$ by $\mathcal{H}$ is exactly $\mathcal{H}(\mathbb{F}_{q^2})$, the set of $\mathbb{F}_{q^2}$-rational points of the Hermitian curve, all with ramification index $q^2 - q + 1$. Moreover, the points of $\mathcal{X}$ above $\mathcal{H}(\mathbb{F}_{q^2})$ are precisely the $\mathbb{F}_{q^2}$-rational points of $\mathcal{X}$. Therefore, we immediately obtain that

$$(dy)_{\mathcal{X}} = (q^4 - 2q^3 + q^2 - 2)P_\infty + (q^2 - q) \sum_{P \in \mathcal{X}(\mathbb{F}_{q^2}), P \neq P_\infty} P.$$

Thus, from $z^{q^2-q+1} = y^{q^2} - y$ and equation (6),

$$(dz)_{\mathcal{X}} = (-dy/z^{q^2-q})_{\mathcal{X}} = (q^5 - 2q^3 + q^2 - 2)P_\infty.$$

In particular a differential fdz is regular if and only if $f \in L((q^5 - 2q^3 + q^2 - 2)P_\infty) = L((2g(\mathcal{X}) - 2)P_\infty)$. The corollary now follows by applying Proposition 2.3. □

3 The Weierstrass semigroup $H(P)$ for $P \in \mathcal{X}(\mathbb{F}_{q^6}) \setminus \mathcal{X}(\mathbb{F}_{q^2})$

This section is devoted to the proof of Conjecture 2.2 for any prime power q. In particular in this section $P = P_{(a,b,c)}$ will always denote a point in $\mathcal{X}(\mathbb{F}_{q^6}) \setminus \mathcal{X}(\mathbb{F}_{q^2})$. Further we define the semigroup

$$T := \langle q^3 - q + 1, q^3 + 1, q^3 + i(q^4 - q^3 - q^2 + q - 1) \mid i = 0, \ldots, q-1 \rangle.$$

Conjecture 2.2 then simply states that $H(P) = T$. Our proof of the conjecture consists of two main steps. In the first step, we will show that $T \subset H(P)$ by showing that the generators of T are in $H(P)$. In the second step, we show that the number of gaps of the semigroup T (also known as the genus of T) is exactly equal to the genus of $\mathcal{X}$. Once this has been established, the equality $H(P) = T$ will follow immediately, proving Conjecture 2.2.

3.1 $T \subset H(P)$

As before we use the function $\tilde{x}_P$ defined in equation (2) and its divisor in equation (3). Moreover, for $k \in \mathbb{Z}$, we define the k-th Frobenius twist of $\tilde{x}_P$ as the follows:

$$\tilde{x}_P^{(k)} := -a^{q^{2k+1}} - x + b^{q^{2k+1}} y \text{ for } P = P_{(a,b,c)}. \tag{9}$$

Since we assume that $P \in \mathcal{X}(\mathbb{F}_{q^6}) \setminus \mathcal{X}(\mathbb{F}_{q^2})$, equation (3) implies that

$$(\tilde{x}_P^{(1)})_{\mathcal{X}} = q \sum_{\xi^{q^2-q+1}=1} P_{(a^{q^2},b^{q^2},\xi c^{q^2})} + \sum_{\xi^{q^2-q+1}=1} P_{(a^{q^4},b^{q^4},\xi c^{q^4})} - (q^3+1)P_\infty,$$
$$(\tilde{x}_P^{(2)})_{\mathcal{X}} = q \sum_{\xi^{q^2-q+1}=1} P_{(a^{q^4},b^{q^4},\xi c^{q^4})} + \sum_{\xi^{q^2-q+1}=1} P_{(a,b,\xi c)} - (q^3+1)P_\infty. \tag{10}$$

Lemma 3.1. *Let $P = P_{(a,b,c)} \in \mathcal{X}(\mathbb{F}_{q^6}) \setminus \mathcal{X}(\mathbb{F}_{q^2})$ and let $\tilde{f}_i = f_i/\tilde{z}_P^{iq-i+1}$ where*

$$f_i := \frac{(\tilde{x}_P)^{qi} \cdot \tilde{x}_P^{(2)}}{(\tilde{x}_P^{(1)})^i}, \text{ for } i = 1, \ldots, q-1.$$

Then $(\tilde{f}_i)_\infty = (q^3 + i(q^4 - q^3 - q^2 + q - 1))P$ and in particular $q^3 + i(q^4 - q^3 - q^2 + q - 1) \in H(P)$ for $i = 1, \ldots, q-1$.

Proof. Using equations (3) and (10), we directly obtain that

$$(f_i)_{\mathcal{X}} = (iq^2+1) \sum_{\xi^{q^2-q+1}=1} P_{(a,b,\xi c)} + (q-i) \sum_{\xi^{q^2-q+1}=1} P_{(a^{q^4},b^{q^4},\xi c^{q^4})} - (q^3+1)(iq-i+1)P_\infty.$$

Now using the divisor of $\tilde{z}_P$ given in equation (7), we find that

$$(\tilde{f}_i)_{\mathcal{X}} = -(q^3 + i(q^4 - q^3 - q^2 + q - 1))P + (iq^2+1) \sum_{\substack{\xi^{q^2-q+1}=1, \\ \xi \neq 1}} P_{(a,b,\xi c)} + (q-i) \sum_{\xi^{q^2-q+1}=1} P_{(a^{q^4},b^{q^4},\xi c^{q^4})}.$$

The lemma now follows. □

Note that the lemma is also true for $i = 0$. Considering the corresponding function $\tilde{f}_0 = \tilde{x}_P^{(2)}/\tilde{z}_P$, gives a way to show that $q^3 \in H(P)$. However, this is already known, see equation (8).

Proposition 3.2. *Let $P \in \mathcal{X}(\mathbb{F}_{q^6}) \setminus \mathcal{X}(\mathbb{F}_{q^2})$. Then $T \subset H(P)$.*

Proof. Equation (8) and Lemma 3.1 imply that $\{q^3-q+1, q^3+1, q^3+i(q^4-q^3-q^2+q-1) \mid i = 0, \ldots, q-1\} \subset H(P)$. Since by definition these numbers generate T, the proposition follows. □

3.2 The genus of the numerical semigroup T equals $g(\mathcal{X})$

We now show that the genus $g(T)$ of the numerical semigroup $T = \langle q^3-q+1, q^3+1, q^3+i(q^4-q^3-q^2+q-1) \mid i = 0, \ldots, q-1\rangle$ is equal to $g(\mathcal{X}) = (q^5-2q^3+q^2)/2$. In this way, since we already know that $T \subseteq H(P_{(a,b,c)})$ from Proposition 3.2, Conjecture 2.2 will be completely proved. We recall that a numerical semigroup is called *telescopic* if it is generated by a telescopic sequence, that is by a sequence $(a_1, \ldots, a_k)$ such that

- $\gcd(a_1, \ldots, a_k) = 1$;
- for each $i = 2, \ldots, k$, $a_i/d_i \in \langle a_1/d_{i-1}, \ldots, a_{i-1}/d_{i-1}\rangle$, where $d_i = \gcd(a_1, \ldots, a_i)$ and $d_0 = 0$;

see [8]. From [7, Proposition 5.35], the genus of a semigroup Γ generated by a telescopic sequence $(a_1, \ldots, a_k)$ is

$$g(\Gamma) = \frac{1}{2}\left(1 + \sum_{i=1}^{k}\left(\frac{d_{i-1}}{d_i} - 1\right)a_i\right). \tag{11}$$

For the semigroup S defined by $S := \langle q^3 - q + 1, q^3 + 1\rangle$ we obtain the following:

Lemma 3.3. *The numerical semigroup $S = \langle q^3 - q + 1, q^3 + 1\rangle$ is telescopic. Its genus $g(S)$ is given by*

$$g(S) = \frac{q^3(q^3 - q)}{2}.$$

Proof. Let $a_1 = q^3 - q + 1$ and $a_2 = q^3 + 1$. Then $gcd(a_1, a_2) = 1$ and, using the same notation as above, $d_1 = a_1$ and $d_2 = 1$. Since $a_2/d_2 \in \langle 1\rangle = \langle a_1/d_1\rangle$, S is telescopic. Thus from equation (11),

$$g(S) = \frac{1}{2}\left(1 - a_1 + (a_1 - 1)a_2\right) = \frac{q^3(q^3 - q)}{2}.$$

□

Now the idea is to compute the number of gaps of T by identifying the elements of T that are gaps of S. The following observation is trivial, but will be very useful.

Observation 3.4. *For any integer n, there exist unique integers a and b such that $n = a(q^3-q+1)+b(q^3+1)$ and $0 \le b \le q^3 - q$. An integer n is an element of the semigroup $S = \langle q^3 - q + 1, q^3 + 1\rangle$ if and only if there exist integers a and b such that $n = a(q^3 - q + 1) + b(q^3 + 1)$, $a \ge 0$ and $0 \le b \le q^3 - q$.*

In the following lemma, we identify several elements of $T \setminus S$ that turn out to play an important role.

Lemma 3.5. *For any $i = 0, \ldots, q - 1$ and $j = 1, \ldots, q - 1$, define the set*

$$S_{i,j} := \{(iq - jq^2 + k_1)(q^3 - q + 1) + (jq^2 - i + k_2)(q^3 + 1) \mid k_1 = 0, \ldots, q - 1,\ k_2 = 0, \ldots, q^3 - q - jq^2 + i\}.$$

Then we have:

1. $S_{i,j} \subset T \setminus S$.
2. $S_{i,j} \cap S_{i'j'} = \emptyset$ *if* $(i', j') \neq (i, j)$, $0 \le i' \le q - 1$ *and* $1 \le j' \le q - 1$.
3. $|S_{i,j}| = q(q^3 - q - jq^2 + i + 1)$.

Proof. First of all note that

$$jq^3 + i(q^4 - q^3 - q^2 + q - 1) = (-jq^2 + iq)(q^3 - q + 1) + (jq^2 - i)(q^3 + 1).$$

Using this, it is clear from Proposition 3.2, that $(iq - jq^2 + k_1)(q^3 - q + 1) + (jq^2 - i + k_2)(q^3 + 1) \in T$ for any i, j, k_1, k_2 in the given range. To show that these elements are not in S, observe that

$$iq - jq^2 + k_1 \le (q - 1)q - q^2 + q - 1 < 0 \text{ and } 0 \le jq^2 - i + k_2 \le q^3 - q. \tag{12}$$

Observation 3.4 now implies that $(iq - jq^2 + k_1)(q^3 - q + 1) + (jq^2 - i + k_2)(q^3 + 1) \notin S$. This completes the proof of the first item.

Now suppose that $S_{i,j} \cap S_{i'j'} \neq \emptyset$. Then there exist integers k_1, k_1', k_2, k_2' satisfying the defining requirements of $S_{i,j}$ and $S_{i'j'}$ such that

$$(iq - jq^2 + k_1)(q^3 - q + 1) + (jq^2 - i + k_2)(q^3 + 1) = (i'q - j'q^2 + k_1')(q^3 - q + 1) + (j'q^2 - i' + k_2')(q^3 + 1).$$

As above, we have equation (12) as well as the similar equation

$$i'q - j'q^2 + k_1' < 0 \text{ and } 0 \leq j'q^2 - i' + k_2' \leq q^3 - q.$$

Observation 3.4 therefore implies that

$$iq - jq^2 + k_1 = i'q - j'q^2 + k_1' \text{ and } jq^2 - i + k_2 = j'q^2 - i' + k_2',$$

and in particular $(i - i')q - (j - j')q^2 + (k_1 - k_1') = 0$. Considering this equation modulo q and modulo q^2, we see that $k_1 = k_1'$ and $i = i'$, implying that $j = j'$ as well. Then it is also clear that $k_2 = k_2'$. This implies the second item.

As for the third item: if

$$(iq - jq^2 + k_1)(q^3 - q + 1) + (jq^2 - i + k_2)(q^3 + 1) = (iq - jq^2 + k_1')(q^3 - q + 1) + (jq^2 - i + k_2')(q^3 + 1),$$

with integers k_1, k_1', k_2, k_2' satisfying the defining requirements of $S_{i,j}$, then the same reasoning as in above proof of the second item, shows that $k_1 = k_1'$ and $k_2 = k_2'$. Hence the cardinality of $S_{i,j}$ is simply the number of possibilities for k_1 times that for k_2. □

Picture 3.2 describes the sets $S_{i,j}$ for $q = 3$. In this picture a point of coordinates (a, b) is used to represent the element $a(q^3 - q + 1) + b(q^3 + 1)$. Black dots represent elements of the numerical semigroup S, while white dots represent the elements contained in $S_{i,j}$ for some i and j.

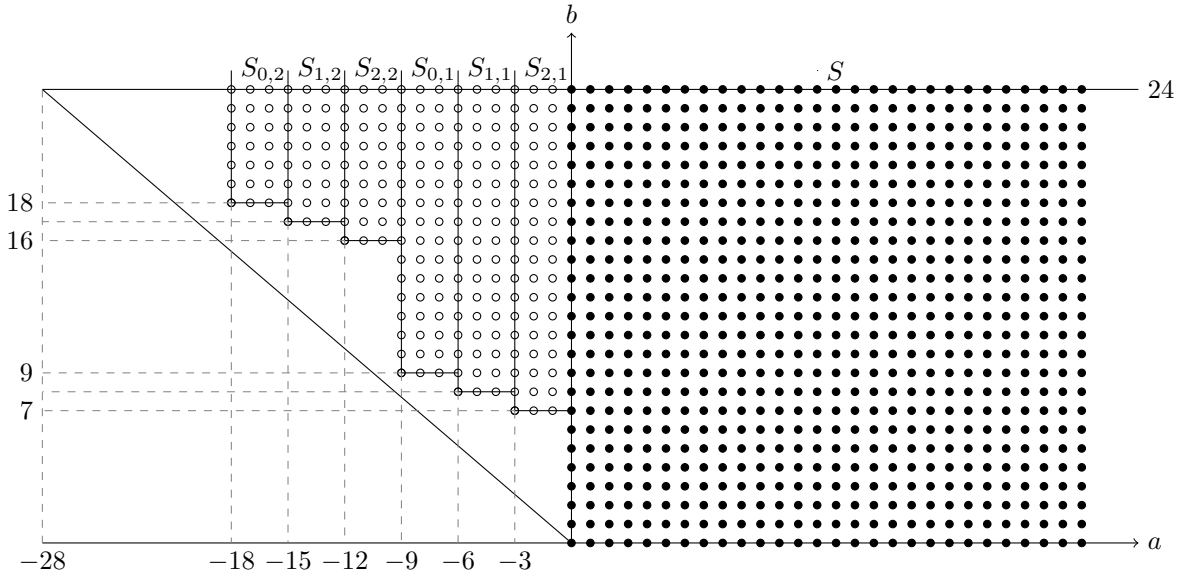

Figure 1: The sets $S_{i,j}$ and S for $q = 3$
○: Elements in $S_{i,j}$ ●: Elements in S

We are now ready to prove Conjecture 2.2.

Theorem 3.6. *We have $g(T) = g(\mathcal{X})$ and in particular $H(P) = T$.*

Proof. Proposition 3.2 implies that $g(T) \geq g(\mathcal{X})$. Hence the theorem follows once we show that $g(T) \leq g(\mathcal{X})$. However, using the first two items of Lemma 3.5, we see that

$$g(T) \leq g(S) - \sum_{i=0}^{q-1}\sum_{j=1}^{q-1} |S_{i,j}|.$$

Using Lemma 3.3 and item three of Lemma 3.5 we obtain

$$\begin{aligned} g(T) &\leq \frac{q^6-q^4}{2} - \sum_{i=0}^{q-1}\sum_{j=1}^{q-1} q(q^3-q+1-jq^2+i) \\ &= \frac{q^6-q^4}{2} - \sum_{i=0}^{q-1}\sum_{j=1}^{q-1} q(q^3-q+1) + \sum_{i=0}^{q-1}\sum_{j=1}^{q-1} jq^3 - \sum_{i=0}^{q-1}\sum_{j=1}^{q-1} iq \\ &= \frac{q^6-q^4}{2} - q^2(q-1)(q^3-q+1) + \frac{q^5(q-1)}{2} - \frac{q^2(q-1)^2}{2} = \frac{q^5-2q^3+q^2}{2} = g(\mathcal{X}). \end{aligned}$$

□

A direct consequence of the above theorem is that $H(P) = \left(\bigcup_{i,j} S_{i,j}\right) \cup S$. It is not hard to obtain more information about $H(P)$ from the above calculations. For example, it is clear that the multiplicity of $H(P)$ (i.e., the smallest positive element in $H(P)$) is equal to q^3-q+1, while its conductor (i.e., the largest gap) is $2g(\mathcal{X})-1$. This means in particular that like $H(P_\infty)$, the semigroup $H(P)$ is symmetric. Since $H(P_\infty)$ has multiplicity q^3-q^2+q, we also see that $H(P) \neq H(P_\infty)$.

4 The Weierstrass semigroup $H(P)$ for $P \notin \mathcal{X}(\mathbb{F}_{q^6})$

In this section we determine the Weierstrass semigroup $H(P)$ for $P \notin \mathcal{X}(\mathbb{F}_{q^6})$. In particular in this section $P = P_{(a,b,c)}$ will always denote a point on $\mathcal{X}$ not in $\mathcal{X}(\mathbb{F}_{q^6})$. For future reference, note that as in the previous section, this means that $c \neq 0$. As we will see, the semigroup $H(P)$ is the same for all $P \notin \mathcal{X}(\mathbb{F}_{q^6})$ and hence the 'generic' semigroup for a point on $\mathcal{X}$. Our approach is use Corollary 2.4 to construct gaps of $H(P)$ by computing the valuation at P of functions $f \in L((2g(\mathcal{X})-2)P_\infty)$. It is very easy to find a basis of the Riemann–Roch space $L((2g(\mathcal{X})-2)P_\infty)$. For example the functions $x^i y^j z^k$ where $i \geq 0$, $0 \leq j \leq q$, $0 \leq k \leq q^2+q$ and $i(q^3+1)+j(q^3-q^2+q)+kq^3 \leq 2g(\mathcal{X})-2$ form a basis. However, this does not settle the matter, since these basis elements all will have valuation 0 at P. Therefore an effort must be made to construct functions in $L((2g(\mathcal{X})-2)P_\infty)$ having distinct valuations at P. In the next subsection, we construct functions with various valuations at P. After that we will combine these functions and obtain a set G of several explicitly described gaps of $H(P)$ using Corollary 2.4. The remainder of the section will then be a somewhat lengthy calculation showing that the set G in fact contains $g(\mathcal{X})$, and hence all, gaps of $H(P)$.

4.1 Construction of functions.

We start by constructing a function g_1 with small, but positive, valuation at $P = P_{(a,b,c)}$. It will be convenient to define $\beta = b^{q^2} - b$. Note that $b^{q^2} - b = c^{q^2-q+1} \neq 0$, since $P \notin \mathcal{X}(\mathbb{F}_{q^6})$ (and therefore a fortiori $P \notin \mathcal{X}(\mathbb{F}_{q^2})$). We define

$$g_1 := (\beta^{q^2-1} - 1)\tilde{x}_P^q + \beta^{q^2+q} + \beta^q \left((\tilde{y}_P - \beta)(\tilde{x}_P + \beta^q(\tilde{y}_P - \beta))^{q-1}\right).$$

The functions $\tilde{x}_P$ and $\tilde{y}_P$ are as in equation (2). This definition may seen ad hoc, but it arises naturally when constructing functions of low pole order at P_∞ and large vanishing order at P. More precisely, we have the following lemma.

Lemma 4.1. *The function g_1 is an element of $L((2g(\mathcal{X}) - 2)P_\infty)$. Moreover $v_{P_\infty}(g_1) \geq -q(q^3+1)$ and $v_P(g_1) = q^2 + 1$.*

Proof. It is clear that g_1 only can have a pole at P_∞. Moreover, from equations (3) and (4) imply that $\tilde{x}_P$ (resp. $\tilde{y}_P$) has a pole at P_∞ of order q^3+1 (resp. $q^3 - q^2 + q$). Therefore, the triangle inequality implies that $v_{P_\infty}(g_1) \geq v_{P_\infty}(\tilde{x}_P^q) = -q(q^3+1)$, which is what we want to show.

From equation (4), we see that the function $\tilde{y}_P$ is a local parameter for the point $P = P_{(a,b,c)}$. The defining equation for $\mathcal{H}_q$ directly implies that $\tilde{x}_P^q + \tilde{x}_P = \beta\tilde{y}_P^q - \tilde{y}_P^{q+1}$. Hence we easily can obtain the power series development of $\tilde{x}_P$ in terms of $\tilde{y}_P$. More precisely, we obtain that

$$\begin{aligned}\tilde{x}_P &= \beta\tilde{y}_P^q - \tilde{y}_P^{q+1} - \tilde{x}_P^q = \beta\tilde{y}_P^q - \tilde{y}_P^{q+1} - \beta^q\tilde{y}_P^{q^2} + \tilde{y}_P^{q^2+q} + \cdots \\ &= (\tilde{y}_P - \beta)(-\tilde{y}_P^q + (\tilde{y}_P - \beta)^{q-1}\tilde{y}_P^{q^2}) + \cdots \end{aligned} \tag{13}$$

Using this, we also obtain that

$$\begin{aligned}(\tilde{y}_P - \beta)\left(\tilde{x}_P + \beta^q(\tilde{y}_P - \beta)\right)^{q-1} &= (\tilde{y}_P - \beta)\left((\tilde{y}_P - \beta)(-\tilde{y}_P^q + (\tilde{y}_P - \beta)^{q-1}\tilde{y}_P^{q^2}) + \beta^q(\tilde{y}_P - \beta)\right)^{q-1} + \cdots \\ &= (\tilde{y}_P - \beta)^q\left(-(\tilde{y}_P - \beta)^q + (\tilde{y}_P - \beta)^{q-1}\tilde{y}_P^{q^2}\right)^{q-1} + \cdots \\ &= (\tilde{y}_P - \beta)^{q^2-q+1}\left(-(\tilde{y}_P - \beta) + \tilde{y}_P^{q^2}\right)^{q-1} + \cdots \\ &= (\tilde{y}_P - \beta)^{q^2} - (\tilde{y}_P - \beta)^{q^2-1}\tilde{y}_P^{q^2} + \cdots \\ &= -\beta^{q^2} + (1 - \beta^{q^2-1})\tilde{y}_P^{q^2} + \beta^{q^2-2}\tilde{y}_P^{q^2+1} + \cdots . \end{aligned} \tag{14}$$

Combining equations (13) and (14), we see that

$$\begin{aligned} g_1 &= (\beta^{q^2-1} - 1)\beta^q\tilde{y}_P^{q^2} + \beta^{q^2+q} + \beta^q(-\beta^{q^2} + (1 - \beta^{q^2-1})\tilde{y}_P^{q^2} + \beta^{q^2-2}\tilde{y}_P^{q^2+1}) + \cdots \\ &= \beta^{q^2+q-2}\tilde{y}_P^{q^2+1} + \cdots \end{aligned}$$

This implies that $v_P(g_1) = q^2 + 1$, which is what we wanted to show. □

The next functions are inspired by the previous section in the sense that we again use the functions $\tilde{x}_P^{(k)}$ introduced in equation (9), but now for $P = P_{(a,b,c)} \notin \mathcal{X}(\mathbb{F}_{q^6})$. For $s = 1, \ldots, q-2$ we define

$$h_s := \left(\frac{\tilde{x}_P^q}{\tilde{x}_P^{(1)}}\right)^{s+1} \cdot \tilde{x}_P^{(2)}.$$

We have the following lemma about these functions.

Lemma 4.2. *Let $s = 1, \dots, q-2$. The function h_s is an element of $L((2g(\mathcal{X})-2)P_\infty)$. Moreover $v_{P_\infty}(h_s) = -(q(s+1)-s)(q^3+1)$ and $v_P(h_s) = (s+1)q^2$.*

Proof. Using equations (3) and (10), we see that $v_{P_\infty}(h_s) = -(q(s+1)-s)(q^3+1)$ and that h_s has no other poles. Further it is well known that $\mathcal{H}_q(\mathbb{F}_{q^2}) = \mathcal{H}_q(\mathbb{F}_{q^4})$. Since any point in $\mathcal{H}_q(\mathbb{F}_{q^2})$ ramifies totally in the cover $\mathcal{X} \to \mathcal{H}$, this means that also $\mathcal{X}(\mathbb{F}_{q^2}) = \mathcal{X}(\mathbb{F}_{q^4})$. Therefore $v_P(\tilde{x}_P^{(2)}) = 0$, since $P \notin \mathcal{X}(\mathbb{F}_{q^6})$. This implies that

$$v_P(h_s) = (s+1)\left(qv_P(\tilde{x}_P) - v_P(\tilde{x}_P^{(1)})\right) = (s+1)q^2,$$

as claimed. □

Now we able to determine several gaps of $H(P)$.

Proposition 4.3. *Let $P \notin \mathcal{X}(\mathbb{F}_{q^6})$ be a point on $\mathcal{X}$. Then*

$$G := \{iq^3 + j + kq + m(q^2+1) + \sum_{s=1}^{q-2} n_s((s+1)q^2) + 1 \mid i,j,k,m,n_1,\dots,n_{q-2} \in \mathbb{Z}_{\geq 0}, \text{ and}$$
$$i(q+1) + jq + k(q+1) + mq(q+1) + \sum_{s=1}^{q-2} n_s((s+1)q - s)(q+1) \leq (q+1)(q^2-2)\},$$

is a set of gaps at P.

Proof. Let $i,j,k,m,n_1,\dots,n_{q-2}$ be nonnegative integers and write $f = \tilde{z}_P^i \tilde{y}_P^j \tilde{x}_P^k g_1^m \prod_{s=1}^{q-2} h_s^{n_s}$. Equations (3), (4), (5) combined with Lemmas 4.1 and 4.2 imply that $f \in L((2g(\mathcal{X})-2)P_\infty)$ if

$$i(q^3+1) + j(q^3-q^2+q) + k(q^3+1) + m(q^4+q) + \sum_{s=1}^{q-2} n_s((s+1)q-s)(q^3+1) \leq q^5 - 2q^3 + q^2 - 2,$$

which is equivalent to

$$i(q+1) + jq + k(q+1) + mq(q+1) + \sum_{s=1}^{q-2} n_s((s+1)q-s)(q+1) \leq (q+1)(q^2-2). \tag{15}$$

On the other hand we have

$$v_P(f) = iq^3 + j + kq + m(q^2+1) + \sum_{s=1}^{q-2} n_s((s+1)q^2).$$

Hence the claim follows from Lemma 2.4. □

Observation 4.4. *Inequality (16) implies in particular that $i \leq q^2-2, j \leq q^2+q-3, k \leq q^2-2$, $m \leq q-1$ and $n_s \leq \lfloor (q+1)/(s+1) \rfloor$. This implies directly that the largest gap of $H(P)$ that is contained in G is obtained by putting $i = q^2-2$ and all other remaining variables to 0. In other words: the largest element in G is $q^5 - 2q^3 + 1 = 2g(\mathcal{X}) - q^2 + 1$.*

Observation 4.5. *If $j \geq q$ and the tuple $(i, j, k, m, n_1, \ldots, n_{q-2})$ satisfies inequality* (16)*, then the tuple $(i, j-q, k+1, m, n_1, \ldots, n_s)$ will also satisfy inequality* (16)*. This implies that when calculating the set G, we may assume that $j \leq q-1$. Moreover, inequality* (15) *is equivalent to*

$$i + j + k + mq + \sum_{s=1}^{q-2} n_s((s+1)q - s) \leq q^2 - 2 + \frac{j}{q+1},$$

which for $j \leq q-1$ is equivalent to

$$i + j + k + mq + \sum_{s=1}^{q-2} n_s((s+1)q - s) \leq q^2 - 2, \tag{16}$$

since all variables involved are integers.

4.2 $|G| = g(\mathcal{X})$.

We now prove that G is exactly the set of gaps G at $P = P_{(a,b,c)} \notin \mathcal{X}(\mathbb{F}_{q^6})$, that is $|G| = g(\mathcal{X})$. Since we already know that G contains gaps of $H(P)$, it is sufficient to show that $|G| \geq g(\mathcal{X})$. This will require a detailed study of the elements of G. To this end we consider the following map

$$\varphi : \mathbb{Z}_{\geq 0}^{q+2} \to \mathbb{Z}_{\geq 0}, \quad \text{with} \quad \varphi(i, j, k, m, n_1, \ldots, n_{q-2}) = iq^3 + j + kq + m(q^2+1) + \sum_{s=1}^{q-2} n_s((s+1)q^2) + 1,$$

and consider the set

$$\mathcal{G} = \{(i, j, k, m, n_1, \ldots, n_{q-2}) \in \mathbb{Z}_{\geq 0}^{q+2} \mid j \leq q-1, \text{ inequality (16) holds}\}.$$

Then by Observation 4.5 we have $G = \varphi(\mathcal{G})$. The main difficulty is that $\varphi_{|\mathcal{G}}$, the restriction of the map φ to $\mathcal{G}$, is not injective. This makes estimating the cardinality of G somewhat tricky. We proceed by studying the image of φ on the following three subsets of $\mathcal{G}$.

$$\mathcal{G}_1 := \{(i, 0, k, m, 0, \ldots, 0) \in \mathcal{G}\},$$
$$\mathcal{G}_2 := \{(i, j, k, m, 0, \ldots, 0) \in \mathcal{G} \mid 1 \leq j \leq q-1, k \leq q-1, j+m \leq q-1\}$$
$$\mathcal{G}_3 := \{(i, j, k, 0, \ldots, 0, n_s, 0, \ldots, 0) \in \mathcal{G} \mid k \leq q-1, 1 \leq s \leq q-2, n_s = 1, i+k+(s+1)q \geq q^2-1\}.$$

Further, we write $G_1 = \varphi(\mathcal{G}_1)$, $G_2 = \varphi(\mathcal{G}_2)$ and $G_3 = \varphi(\mathcal{G}_3)$. We will show that these sets are mutually disjoint and that their cardinalities add up to $|G|$ in a series of lemmas.

Lemma 4.6. *Let $\mathcal{G}_1$ and $G_1 = \varphi(\mathcal{G}_1)$ be as above. Then φ restricted to $\mathcal{G}_1$ is injective and*

$$|G_1| = \frac{1}{2}q^2(q-1)\left(\frac{1}{3}q^2 + \frac{5}{6}q + \frac{1}{2}\right).$$

Proof. If $(i, 0, k, m, 0, \ldots, 0) \in \mathcal{G}_1$, then $\varphi(i, 0, k, m, 0, \ldots, 0) = iq^3 + kq + m(q^2+1) + 1$ and by inequality (16) $i + k + mq \leq q^2 - 2$. This implies in particular that

$$0 \leq m \leq q-1 \text{ and } 0 \leq kq + m(q^2+1) \leq (k+mq)q + q - 1 \leq (q^2-2)q + q - 1 < q^3.$$

Now suppose $(i_1,0,k_1,m_1,0,\dots,0),(i_2,0,k_2,m_2,0,\dots,0)\in\mathcal{G}_1$ and

$$i_1q^3+k_1q+m_1(q^2+1)=i_2q^3+k_2q+m_2(q^2+1).$$

Calculating modulo q and using that $0\le m_1\le q-1$ and $0\le m_2\le q-1$ (see Observation 4.5), we see that $m_1=m_2$. Further, since $0\le k_1q+m_1(q^2+1)<q^3$ and $0\le k_2q+m_2(q^2+1)<q^3$, we see that $k_1q+m_1(q^2+1)=k_2q+m_2(q^2+1)$ and $i_1q^3=i_2q^3$. Combining these equalities, we see that $(i_1,0,k_1,m_1,0,\dots,0)=(i_2,0,k_2,m_2,0,\dots,0)$, which is what we wanted to show.

Now we compute $|G_1|$. First of all, from the above we see that $|G_1|=|\mathcal{G}_1|$. Further we have

$$\begin{aligned}|\mathcal{G}_1|&=\sum_{m=0}^{q-1}\sum_{i=0}^{q^2-2-mq}\sum_{k=0}^{q^2-2-mq-i}1=\sum_{m=0}^{q-1}\sum_{i=0}^{q^2-2-mq}(q^2-1-mq-i)\\&=\sum_{m=0}^{q-1}\frac{(q^2-1-mq)(q^2-mq)}{2}=\frac{(q^2-1)q^3}{2}+\sum_{m=0}^{q-1}\frac{-2q^3-q^2+q}{2}m+\binom{m+1}{2}q^2\\&=\frac{(q^2-1)q^3}{2}+\frac{-2q^3-q^2+q}{2}\binom{q}{2}+\binom{q+1}{3}q^2.\end{aligned}$$

In the last equality we used *summation on the upper index* to evaluate the summation $\sum_m\binom{m+1}{2}$; see [5, Eqn. (5.10)]. The desired equality for $|G_1|$ now follows. □

Lemma 4.7. *Let $\mathcal{G}_2$ and $G_2=\varphi(\mathcal{G}_2)$ be as above. Then φ restricted to $\mathcal{G}_2$ is injective and*

$$|G_2|=\frac{1}{2}q^2(q-1)\left(\frac{2}{3}q^2-\frac{1}{6}q-\frac{5}{6}\right).$$

Proof. If $(i,j,k,m,0,\dots,0)\in\mathcal{G}_2$, then $\varphi(i,j,k,m,0,\dots,0)=iq^3+j+kq+m(q^2+1)+1$ and by definition we have $1\le j\le q-1$, $1\le j+m\le q-1$ and $0\le k\le q-1$. Moreover, inequality (16) gives that $i+j+k+mq\le q^2-2$. Similarly as in the previous lemma, we obtain that

$$0\le m\le q-1 \text{ and } 0\le j+kq+m(q^2+1)\le(k+mq)q+q-1\le(q^2-2)q+q-1<q^3.$$

Now suppose $(i_1,j_1,k_1,m_1,0,\dots,0),(i_2,j_2,k_2,m_2,0,\dots,0)\in\mathcal{G}_2$ and

$$i_1q^3+j_1+k_1q+m_1(q^2+1)=i_2q^3+j_2+k_2q+m_2(q^2+1).$$

Reasoning exactly as in the previous lemma, we obtain that $j_1+m_1=j_2+m_2$, $j_1+k_1q+m_1(q^2+1)=j_2+k_2q+m_2(q^2+1)$ and $i_1=i_2$. Combining the first two equations, we deduce that $k_1q+m_1q^2=k_2q+m_2q^2$. Since $0\le k_1\le q-1$ and $0\le k_2\le q-1$, we see $k_1=k_2$, which now implies that $(i_1,j_1,k_1,m_1,0,\dots,0)=(i_2,j_2,k_2,m_2,0,\dots,0)$.

Now we compute $|G_2|$. First note that $k\le q-1$, but for a given j and m, we also have $k\le q^2-2-j-mq$. However, since $j\ge1$ and $0\le j+m\le q-1$, we see that $m\le q-2$. Hence $q^2-2-j-mq\ge q^2-2-1-(q-2)q\ge$

$q-1$, implying that the condition $k \le q^2-2-j-mq$ is trivially satisfied. Hence

$$\begin{aligned}|\mathcal{G}_2| &= \sum_{j=1}^{q-1}\sum_{m=0}^{q-1-j}\sum_{k=0}^{q-1}\sum_{i=0}^{q^2-2-j-k-mq} 1 = \sum_{j=1}^{q-1}\sum_{m=0}^{q-1-j}\sum_{k=0}^{q-1}(q^2-1-j-k-mq)\\ &= \sum_{j=1}^{q-1}\sum_{m=0}^{q-1-j}(q^2-1-j-mq)q - \binom{q}{2} = \sum_{j=1}^{q-1}\left((q^2-1-j)q-\binom{q}{2}\right)(q-j) - q^2\binom{q-j}{2}\\ &= \sum_{j=1}^{q-1}\left((q^2-q)q-\binom{q}{2}\right)(q-j) - (q^2-2q)\binom{q-j}{2} = \left((q^2-q)q-\binom{q}{2}\right)\binom{q}{2} - (q^2-2q)\binom{q}{3}.\end{aligned}$$

The desired equality now follows. □

Lemma 4.8. *Let $\mathcal{G}_3$ and $G_3 = \varphi(\mathcal{G}_3)$ be as above. Then φ restricted to $\mathcal{G}_3$ is injective and*

$$|G_3| = \frac{1}{2}q^2(q-1)\left(\frac{1}{3}q-\frac{2}{3}\right).$$

Proof. If $(i,j,k,0,0,\ldots,0,n_s,0,\ldots,0) \in \mathcal{G}_3$, then $\varphi(i,j,k,0,0,\ldots,0,n_s,0,\ldots,0) = iq^3+j+kq+(s+1)q^2+1$ and by definition we have $n_s = 1$, $1 \le s \le q-2$, $0 \le j \le q-1$, $0 \le k \le q-1$ and $i+k+(s+1)q \ge q^2-1$ (that is $i+k+sq \ge q^2-q-1$). Moreover, inequality (16) gives that $i+j+k+s(q-1) \le q^2-q-2$. Note that the inequalities $i+k+sq \ge q^2-q-1$ and $i+j+k+s(q-1) \le q^2-q-2$ only can be satisfied simultaneously, if $j \le s-1$, so we may assume this as well in the remainder of the proof.

Now suppose $(i_1,j_1,k_1,0,0,\ldots,0,n_s,0,\ldots,0), (i_1,j_1,k,0,0,\ldots,0,1,0,\ldots,0) \in \mathcal{G}_3$ and

$$i_1q^3 + j_1 + k_1q + (s_1+1)q^2 = i_2q^3 + j_2 + k_2q + (s_2+1)q^2.$$

Since the q-ary expansion of a number is unique, we immediately obtain that $j_1 = j_2$, $k_1 = k_2$ and $s_1 = s_2$, since all variables involved at between 0 and $q-1$. Hence $i_1 = i_2$ as well and the first part of the lemma follows.

Now we compute $|G_3|$. Recall that we may assume $j \le s-1$. Hence

$$\begin{aligned}|\mathcal{G}_3| &= \sum_{s=1}^{q-2}\sum_{j=0}^{s-1}\sum_{k=0}^{q-1}\sum_{i=q^2-q-1-k-sq}^{q^2-q-2-j-k-s(q-1)} 1 = \sum_{s=1}^{q-2}\sum_{j=0}^{s-1}\sum_{k=0}^{q-1}(s-j)\\ &= q\sum_{s=1}^{q-2}\sum_{j=0}^{s-1}(s-j) = q\sum_{s=1}^{q-2}\binom{s+1}{2} = q\binom{q}{3}.\end{aligned}$$

The desired equality now follows. □

Finally to obtain an estimate for $|G|$, we need to study the intersections of the sets G_1, G_2 and G_3. It turns out that they are disjoint, as we will now show.

Lemma 4.9. *The sets G_1, G_2 and G_3 defined above are mutually disjoint.*

Proof. **Part 1.** $G_1 \cap G_2 = \emptyset$**.** Let $(i_1, 0, k_1, m_1, 0, \ldots, 0) \in \mathcal{G}_1$, $(i_2, j_2, k_2, m_2, 0, \ldots, 0) \in \mathcal{G}_2$ and suppose that

$$i_1 q^3 + k_1 q + m_1(q^2+1) = i_2 q^3 + j_2 + k_2 q + m_2(q^2+1).$$

Since $0 \leq m_1 \leq q-1$ and $1 \leq j_2 + m_2 \leq q-1$, we see that $m_1 = j_2 + m_2$ and hence that $i_1 q^2 + k_1 + m_1 q = i_2 q^2 + k_2 + m_2 q$. Note that $m_1 - m_2 = j_2 \geq 0$, where the inequality follows from the definition of $\mathcal{G}_2$. Inequality (16) implies that $k_1 + m_1 q < q^2$ as well as $k_2 + m_2 q < q^2$. Hence we obtain $i_1 = i_2$ and $k_1 + m_1 q = k_2 + m_2 q$, whence $(m_1 - m_2)q = k_2 - k_1$. This implies that $k_1 \equiv k_2 \pmod{q}$, but since $k_1 \geq 0$ and $0 \leq k_2 \leq q-1$ we can deduce $k_1 - k_2 \geq 0$. On the other hand we already have seen that $m_1 - m_2 = j_2 \geq 1$, but then we arrive at a contradiction, since $0 < (m_1 - m_2)q = k_2 - k_1 \leq 0$.

Part 2. $G_1 \cap G_3 = \emptyset$**.** Let $(i_1, 0, k_1, m_1, 0, \ldots, 0) \in \mathcal{G}_1$, $(i_3, j_3, k_3, 0, 0, \ldots, 0, 1, 0, \ldots, 0) \in \mathcal{G}_3$ and suppose that

$$i_1 q^3 + k_1 q + m_1(q^2+1) = i_3 q^3 + j_3 + k_3 q + (s+1)q^2.$$

Similarly as in part 1 above, we obtain that $m_1 = j_3$, whence $i_1 q^2 + k_1 + m_1 q = i_3 q^2 + k_3 + (s+1)q$, as well as the inequality $k_1 + m_1 q < q^2$. However, since $k_3 \leq q-1$ and $s+1 \leq q-1$, we also have $k_3 + (s+1)q < q^3$. Therefore we obtain that $i_1 = i_3$ as well as $k_1 + m_1 q = k_3 + (s+1)q$. This implies that

$$i_3 + k_3 + (s+1)q = i_1 + k_1 + m_1 q \leq q^2 - 2,$$

where we have used inequality (16) to obtain the inequality. On the other hand $i_3 + k_3 + (s+1)q \geq q^2 - 1$ by the definition of $\mathcal{G}_3$ and we arrive at a contradiction.

Part 3. $G_2 \cap G_2 = \emptyset$**.** Let $(i_2, j_2, k_2, m_2, 0, \ldots, 0) \in \mathcal{G}_2$, $(i_3, j_3, k_3, 0, 0, \ldots, 0, 1, 0, \ldots, 0) \in \mathcal{G}_3$ and suppose that

$$i_2 q^3 + j_2 + k_2 q + m_2(q^2+1) = i_3 q^3 + j_3 + k_3 q + (s+1)q^2.$$

Reasoning very similarly as in Part 1 and Part 2, we obtain $j_2 + m_2 = j_3$, $i_2 = i_3$ and

$$i_3 + k_3 + (s+1)q = i_2 + k_2 + m_2 q \leq q^2 - 2.$$

Again we arrive at a constriction. □

We are now ready to prove the main theorem of this section.

Theorem 4.10. *Let P be a point of $\mathcal{X}$ with $P \notin \mathcal{X}(\mathbb{F}_{q^6})$. Then the set of gaps of $H(P)$ is given by,*

$$G = \{iq^3 + kq + m(q^2+1) + \sum_{s=1}^{q-2} n_s((s+1)q^2) + j + 1 \mid i, j, k, m, n_1, \ldots, n_{q-2} \in \mathbb{Z}_{\geq 0}, j \leq q-1, \text{ and}$$

$$i + j + k + mq + \sum_{s=1}^{q-2} n_s((s+1)q - s) \leq q^2 - 2\}.$$

Moreover, the set of Weierstrass points W on $\mathcal{X}$ coincides with $\mathcal{X}(\mathbb{F}_{q^6})$.

Proof. Combing Lemmas 4.6, 4.7, 4.8, and 4.9 we see that

$$|G| \geq |G_1| + |G_2| + |G_3| = \frac{1}{2}q^2(q-1)(q^2+q-1) = g(\mathcal{X}).$$

Since we know that $H(P)$ has exactly $g(\mathcal{X})$ gaps, Proposition 4.3 then implies that $H(P) = \mathbb{N} \setminus G$. From Observation 4.4, we deduce that the largest gap in $H(P)$ is $2g(\mathcal{X}) - q^2 + 1$, while we already know that for any $P \in \mathcal{X}(\mathbb{F}_{q^6})$, the largest gap is $2g(\mathcal{X}) - 1$. This implies the last statement in the theorem. □

The proof also shows that the gaps of $H(P)$ are precisely $G_1 \cup G_2 \cup G_3$, which is convenient when checking if a particular number is a gap or not. For example, this allows us to compute the multiplicity (smallest positive element) of $H(P)$ fairly easily.

Corollary 4.11. *Let P be a point of $\mathcal{X}$ with $P \notin \mathcal{X}(\mathbb{F}_{q^6})$. The multiplicity of $H(P)$ is equal to $q^3 - 1$.*

Proof. From Stöhr-Voloch Theory we know that q^3-1 and q^3 are non-gaps at P, since P is not a Weierstrass point; see [6, Proposition 10.9]. It is also not difficult to verify this directly. On the other hand, let $1 \leq a \leq q^3 - 2$ be an integer and write $a - 1 = c_0 + c_1 q + c_2 q^2$ with $0 \leq c_t \leq q - 1$ for $t = 1, 2, 3$. Then we distinguish three cases.
Case 1. $c_2 \geq c_0$ **and** $(c_1, c_2) \neq (q-1, q-1)$**.** In this case a direct verification shows that $a = \varphi(0, 0, c_1 + (c_2 - c_0)q, c_0, 0 \ldots, 0)$ and that $(0, 0, c_1 + (c_2 - c_0)q, c_0, 0 \ldots, 0) \in \mathcal{G}_1$.
Case 2. $c_2 < c_0$**.** We have $a = \varphi(0, c_0 - c_2, c_1, c_2, 0 \ldots, 0)$ and $(0, c_0 - c_2, c_1, c_2, 0 \ldots, 0) \in \mathcal{G}_2$ in this case.
Case 3. $(c_1, c_2) = (q-1, q-1)$ Note that in this case $c_0 \leq q-3$, since $a-1 = c_0+(q-1)q+(q-1)q^2 \leq q^3-3$. One then checks that $a = \varphi(0, c_0, q-1, 0, 0, \ldots, 0, 1)$ and that $(0, c_0, q-1, 0, 0, \ldots, 0, 1) \in \mathcal{G}_3$. □

At this point seems to be reasonable to ask for the generators of the Weierstrass semigroup $H(P)$ for $P \notin \mathcal{X}(\mathbb{F}_{q^6})$. Their explicit determination seems to be a challenging task as the following examples show. In particular the number of generators of $H(P)$ seems to grow quickly with respect to q.

Example 4.12. *Let $P \in \mathcal{X}$ such that $P \notin \mathcal{X}(\mathbb{F}_{q^6})$.*

- *If $q = 2$ then $g = 10$ and*
$$G = \{1, 2, 3, 4, 5, 6, 9, 10, 11, 17\}.$$
Clearly 7 and 8 must be generators of $H(P)$ and since $12 \notin \langle 7, 8\rangle$ and $13 \notin \langle 7, 8, 12\rangle$ we obtain that also 12 and 13 are generators. Note that $\langle 7, 8, 12, 13\rangle \cap \{0, \ldots, 20\} = \{7, 8, 12, 13, 14, 15, 16\}$ and hence also 18 is a generator. In fact
$$H(P) = \langle 7, 8, 12, 13, 18\rangle.$$
Moreover, if $P \in \mathcal{X}$ then
$$H(P) = \begin{cases} \{0, 6, 8, 9, 12, 14, 15, 16, 17, 18, 20, \ldots\}, & \text{if } P \in \mathcal{X}(\mathbb{F}_4), \\ \{0, 7, 8, 9, 13, 14, 15, 16, 17, 18, 20, \ldots\}, & \text{if } P \in \mathcal{X}(\mathbb{F}_{64}) \setminus \mathcal{X}(\mathbb{F}_4), \\ \{0, 7, 8, 12, 13, 14, 15, 16, 18, 19, 20 \ldots\}, & \text{otherwise.} \end{cases}$$

- *If $q = 3$ then $g = 99$ and*
$$G = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 28, 29, 30, 31, 32, 33, 34,$$
$$35, 36, 37, 38, 39, 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 55, 56, 57, 58, 59, 60, 61, 62, 63, 64, 65, 66, 67, 68, 69,$$
$$70, 71, 73, 82, 83, 84, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 109, 110, 111, 112, 113, 114, 115, 116, 118, 119,$$
$$136, 137, 138, 139, 140, 142, 163, 164, 166, 190\}.$$
Arguing as for the previous case, one can prove that
$$H(P) = \langle 26, 27, 50, 51, 72, 74, 75, 96, 97, 117, 120, 121, 141, 145, 165\rangle.$$

It is unclear what the number of generators for general q is. For $q = 4$ the semigroup turns out to have 28 generators.

Collecting the results in the paper, we have proven Theorem 1.1 and Corollary 1.2 from the introduction. We finish by summing up some further facts on the various semigroups on $\mathcal{X}$ in a table, leaving a question mark for the minimal number of generators in the case $P \notin \mathcal{X}(\mathbb{F}_{q^6})$. Determining this number could be interesting future work.

P	multiplicity	conductor	number of generators
$P \in \mathcal{X}(\mathbb{F}_{q^2})$	$q^3 - q^2 + q$	$2g(\mathcal{X}) - 1$	3
$P \in \mathcal{X}(\mathbb{F}_{q^6}) \setminus \mathcal{X}(\mathbb{F}_{q^2})$	$q^3 - q + 1$	$2g(\mathcal{X}) - 1$	$q + 2$
$P \notin \mathcal{X}(\mathbb{F}_{q^6})$	$q^3 - 1$	$2g(\mathcal{X}) - q^2 + 1$	?

Acknowledgments

The first author gratefully acknowledges the support from The Danish Council for Independent Research (Grant No. DFF–4002-00367). The second author would like to thank the Italian Ministry MIUR, Strutture Geometriche, Combinatoria e loro Applicazioni, Prin 2012 prot. 2012XZE22K and GNSAGA of the Italian INDAM.

References

[1] I. Duursma, *Two-Point Coordinate Rings for GK-Curves*, IEEE Trans. Inf. Theory **57**(2), 593-600 (2011).

[2] S. Fanali and M. Giulietti, *One-Point AG Codes on the GK Maximal Curves*, IEEE Trans. Inf. Theory **56**(1), 202–210 (2010).

[3] A. Garcia and P. Viana, Weierstrass points on certain nonclassical curves, Arch. Math. **46**(4), 315-322 (1986).

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

[5] R. Graham, D. E. Knuth, O. Patashnik: *Concrete mathematics. A foundation for computer science.* Second edition. Addison-Wesley Publishing Company, Reading, MA, (1994), xiv+657 pp.

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

[7] T. Høholdt, J. Van Lint, R. Pellikaan, *Algebraic geometry codes*, in: V.S. Pless, W.C. Huffman (Eds.), Handbook of Coding Theory, North-Holland, 871-961 (1998).

[8] C. Kirfel and R. Pellikaan, *The minimum distance of codes in an array coming from telescopic semigroups*, IEEE Trans. Inf. Theory **41**, 1720-1732 (1995).

[9] G. Lachaud, *Sommes dEisenstein et nombre de points de certaines courbes algébriques sur les corps finis*, C.R. Acad. Sci. Paris **305**(Série I) 729-732 (1987).

[10] H. Stichtenoth, *Algebraic function fields and codes*, Springer, 2009.

[11] K.O. Stöhr, J.F. Voloch: *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. **52**(3), 1-19 (1986).

[12] M.A. Tsfasman, G. Vladut, *Algebraic-geometric Codes*, Kluwer, Dordrecht, (1991).

[13] G. D. Villa Salvador, *Topics in the theory of algebraic function fields*, Mathematics: Theory & Applications. Birkhäuser Boston, Inc., Boston, MA, (2006).

Peter Beelen

Technical University of Denmark,
Department of Applied Mathematics and Computer Science,
Matematiktorvet 303B,
2800 Kgs. Lyngby,
Denmark,
pabe@dtu.dk

Maria Montanucci

Universita' degli Studi della Basilicata,
Dipartimento di Matematica, Informatica ed Economia,
Campus di Macchia Romana,
Viale dell' Ateneo Lucano 10,
85100 Potenza,
Italy,
maria.montanucci@unibas.it