On Weierstrass semigroups of some triples on norm-trace curves

Gretchen L. Matthews

Department of Mathematical Sciences, Clemson University, Clemson, SC 29634-0975, USA
gmatthe@clemson.edu,
WWW home page: www.math.clemson.edu/∼gmatthe

Abstract. In this paper, we consider the norm-trace curves which are defined by the equation $y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y = x^{\frac{q^r-1}{q-1}}$ over $\mathbb{F}_{q^r}$ where q is a power of a prime number and $r \geq 2$ is an integer. We determine the Weierstrass semigroup of the triple of points $(P_\infty, P_{00}, P_{0b})$ on this curve.

1 Introduction

Let X be a smooth projective absolutely irreducible curve of genus $g > 1$ over a finite field $\mathbb{F}$, and let $P_1, \ldots, P_m$ be m distinct $\mathbb{F}$-rational points on X. The Weierstrass semigroup $H(P_1, \ldots, P_m)$ of the m-tuple $(P_1, \ldots, P_m)$ is defined by

$$H(P_1, \ldots, P_m) = \left\{ (\alpha_1, \ldots, \alpha_r) \in \mathbb{N}^m : \exists f \in \mathbb{F}(X) \text{ with } (f)_\infty = \sum_{i=1}^{r} \alpha_i P_i \right\},$$

where $\mathbb{F}(X)$ denotes the field of rational functions on X, $(f)_\infty$ denotes the divisor of poles of a rational function f, and $\mathbb{N}$ denotes the set of nonnegative integers. The Weierstrass gap set $G(P_1, \ldots, P_m)$ of the m-tuple $(P_1, \ldots, P_m)$ is defined by

$$G(P_1, \ldots, P_m) = \mathbb{N}^m \setminus H(P_1, \ldots P_m).$$

If $m = 1$, then $H(P_1)$ is the classically studied Weierstrass semigroup and $G(P_1)$ is the classically studied Weierstrass gap sequence (or gap set). It is well known that $|G(P_1)| = g$, the genus of X, regardless of the choice of point P_1. The gap set $G(P_1, P_2)$ was introduced in [1] where the authors note that the cardinality $|G(P_1, P_2)|$ may depend on the choice of points P_1 and P_2. The study of the Weierstrass gap set of a pair was taken up by Kim [9] and later by Homma and Kim [7]. This was soon followed by the works of Ballico and Kim [2] and Ishii [8].

As suggested by Goppa and verified by Garcia, Kim, and Lax for the $m = 1$ case [5], knowledge of Weierstrass semigroups of m-tuples of points provides insight into the parameters of associated algebraic geometry codes. This theme has been explored by a number of authors, including the present [14], [10] as well as Carvalho and Torres [4]. For a recent survey of such results, see [3].

In this paper, we determine a minimal generating set for the Weierstrass semigroup of the triple $(P_\infty, P_{00}, P_{0b})$ on the norm-trace curve $y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y = x^{\frac{q^r-1}{q-1}}$ over $\mathbb{F}_{q^r}$, where $r \geq 2$. Notice that when $r = 2$, the Hermitian curve is obtained. Hence, these results may be viewed as a generalization of some of those in [13] where the Weierstrass semigroup of an m-tuple of collinear points on the Hermitian curve was obtained. This paper may also be seen as a sequel to that of Munuera, Tizziotti, and Torres [15] where the semigroup of the pair (P_∞, P_{00}) on the norm-trace curve is found and then applied to two-point algebraic geometry codes. In fact, we rely heavily on the results contained in both [13] and [15].

This paper is organized as follows. Section 2 provides a background on the Weierstrass semigroup of an m-tuple of points. Section 3 consists of necessary background on the norm-trace curve. The main result of this paper is contained in Section 4.

2 Weierstrass semigroups of m-tuples

In this section, we describe tools useful in the study of Weierstrass semigroups of m-tuples of points. Several generalize those used to study the gap set of a pair of points [9], [7].

We begin with a brief review of notation. The divisor of a rational function f will be denoted by (f), and $\mathbb{Z}^+$ denotes the set of positive integers. Given $a_1, \ldots, a_k \in \mathbb{Z}^+$, the (numerical) semigroup generated by $a_1, \ldots, a_k$ is

$$\langle a_1, \ldots, a_k \rangle := \left\{ \sum_{i=1}^{k} c_i a_i : c_i \in \mathbb{N} \right\}.$$

As usual, given $v \in \mathbb{Z}^r$ where $r \in \mathbb{Z}^+$, the i^{th} coordinate of v is denoted by v_i.

Define a partial order $\preceq$ on $\mathbb{Z}^r$ by $(n_1, \ldots, n_r) \preceq (p_1, \ldots, p_r)$ if and only if $n_i \leq p_i$ for all i, $1 \leq i \leq r$. When comparing elements of $\mathbb{Z}^r$, we will always do so with respect to the partial order $\preceq$.

In [13] it is shown that if $1 \leq m \leq |\mathbb{F}|$, then there exists a minimal subset $\Gamma(P_1, \ldots, P_m) \subseteq H(P_1, \ldots, P_m)$ such that

$$H(P_1, \ldots, P_m) = \{\mathrm{lub}\,\{\mathbf{u_1}, \ldots, \mathbf{u_r}\} \in \mathbb{N}^m : \mathbf{u_1}, \ldots, \mathbf{u_r} \in \Gamma(P_1, \ldots, P_m)\}$$

where

$$\mathrm{lub}\{\mathbf{u_1}, \ldots, \mathbf{u_m}\} = (\max\{\mathbf{u_{1_1}}, \ldots, \mathbf{u_{m_1}}\}, \ldots, \max\{\mathbf{u_{1_m}}, \ldots, \mathbf{u_{m_m}}\}) \in \mathbb{N}^{\mathbf{m}}$$

is least upper bound of the vectors $\mathbf{u_1}, \ldots, \mathbf{u_m} \in \mathbb{N}^{\mathbf{m}}$. In fact, $\Gamma(P_1, \ldots, P_m)$ may be defined as follows.

Definition 1. *Given m $\mathbb{F}$-rational points $P_1, \ldots, P_m$ on a curve over $\mathbb{F}$ where $2 \leq m \leq |\mathbb{F}|$, set*

$$\Gamma(P_1, \ldots, P_m) := \left\{ \mathbf{n} \in \mathbb{N}^m : \begin{array}{l} \mathbf{n} \text{ is minimal in } \{\mathbf{p} \in H(P_1, \ldots, P_m) : p_i = n_i\} \\ \text{for some } i, 1 \leq i \leq m \end{array} \right\}.$$

The set $\Gamma(P_1, \ldots, P_m)$ is called the minimal generating set of the Weierstrass semigroup $H(P_1, \ldots, P_m)$. Hence, to determine the entire Weierstrass semigroup $H(P_1, \ldots, P_m)$, one only needs to determine the minimal generating set $\Gamma(P_1, \ldots, P_m)$.

When $m = 2$,

$$\Gamma\left(P_1, P_2\right) = \{(\alpha, \beta_\alpha) : \alpha \in G(P_1)\}$$

where

$$\beta_\alpha := \min\left\{\beta \in \mathbb{N} : (\alpha, \beta) \in H\left(P_1, P_2\right)\right\}.$$

This set introduced by Kim [9] where he showed that

$$\left\{\beta_\alpha : \alpha \in G\left(P_1\right)\right\} \subseteq G\left(P_2\right)$$

and in fact

$$\begin{array}{rcl} \phi : G\left(P_1\right) & \rightarrow & G\left(P_2\right) \\ \alpha & \mapsto & \beta_\alpha \end{array}$$

is a bijection. While the latter fact fails for $m \geq 3$, we do have the following as proven in [13].

Lemma 1. *If $P_1, \ldots, P_m$ are distinct $\mathbb{F}$-rational points on a curve X over a finite field $|\mathbb{F}|$ and $2 \leq m \leq |\ \mathbb{F}\ |$, then*

$$\Gamma\left(P_1, \ldots, P_m\right) \subseteq G\left(P_1\right) \times \cdots \times G\left(P_m\right).$$

Another property of the minimal generating set that we will rely on is in the following lemma.

Lemma 2. *If $P_1, \ldots, P_m$ are distinct $\mathbb{F}$-rational points on a curve X over a finite field $|\mathbb{F}|$ and $2 \leq m \leq |\ \mathbb{F}\ |$, then*

$$\Gamma\left(P_1, \ldots, P_m\right) = \left\{ \mathbf{n} \in \mathbb{N}^m : \begin{array}{l} \mathbf{n} \text{ is minimal in } \{\mathbf{p} \in H\left(P_1, \ldots, P_m\right) : p_i = n_i\} \\ \text{for all } i, 1 \leq i \leq m \end{array} \right\}.$$

We will use these properties to compute $\Gamma\left(P_1, P_2, P_3\right)$ for the norm-trace curve over $\mathbb{F}_{q^r}$ where $P_1 = P_\infty$, $P_2 = P_{00}$, and $P_3 = P_{0b}$. Before doing so, we discuss relevant properties of the norm-trace curve in the next section.

3 Preliminaries on the norm-trace curve

Let q be a power of a prime number and $r \geq 2$ be an integer. The norm-trace curve X over $\mathbb{F}_{q^r}$ is defined by

$$y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y = x^{a+1}$$

where $a := \frac{q^r-1}{q-1} - 1$. One immediately recognizes that setting $r = 2$ gives the Hermitian curve over $\mathbb{F}_{q^2}$.

In [6], Geil determined that X has q^{2r-1} affine points over $\mathbb{F}_{q^r}$, namely $(\alpha:\beta:1)$ where the norm of α with respect to the extension $\mathbb{F}_{q^r}/\mathbb{F}_q$ is equal to the trace of β with respect to the extension $\mathbb{F}_{q^r}/\mathbb{F}_q$; that is, the set of affine points of X which are rational over $\mathbb{F}_{q^r}$ is

$$\left\{(\alpha:\beta:1) : N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) = Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\beta)\right\}.$$

We will denote such points by $P_{\alpha\beta}$. In addition, X has a single point at infinity P_∞. Note that X has q^{r-1} points of the form $P_{0\beta}$ and $a = q^{r-1}+q^{r-2}+\cdots+q^2+q$. Then the genus of X is given by $g = \frac{a\left(q^{r-1}-1\right)}{2}$.

By exploiting the facts that

$$(x) = \sum_\beta P_{0\beta} - q^{r-1}P_\infty$$

and

$$(y) = (a+1)\,P_{00} - (a+1)\,P_\infty,$$

Geil [6] found that the Weierstrass semigroup of the point at infinity is

$$H(P_\infty) = \left\langle q^{r-1}, a+1\right\rangle.$$

Later, using these same principal divisors, Munuera, Tizziotti, and Torres [15] proved that the Weierstrass semigroup of the point P_{00} is

$$H(P_{00}) =$$

$$\langle a, a+1, qa-1, (2q-1)\,a-2, (3q-2)\,a-3, \ldots, ((\lambda+1)\,q-\lambda)\,a-(\lambda+1)\rangle$$

where $\lambda := a - q^{r-1} - 1 = q^{r-2}+q^{r-3}+\cdots+q-1$.

Now, fix $b \in \mathbb{F}_{q^r}$ with $b^{q^{r-1}} + b^{q^{r-2}} + \cdots + b = 0$. A similar argument to that mentioned above, using the fact that

$$(y-b) = (a+1)\,P_{0b} - (a+1)\,P_\infty,$$

yields

$$H(P_{0b}) = H(P_{00}).$$

Let us use this information to obtain explicit descriptions for elements of the gap sets of the points P_∞ and P_{00}. Some arguments are provided in [15], but we include these details here for easy reference. We claim that the gap set of the point at infinity is

$$G(P_\infty) =$$

$$\left\{\left(q^{r-1}-i+j-1\right)(a+1) - jq^{r-1} : \begin{array}{c} 1 \le j \le i \le a-s \text{ and} \\ (s-1)\,(q-1) \le i-j < s\,(q-1) \\ \text{where } 1 \le s \le a+1-q^{r-1} \end{array}\right\}.$$

Suppose there exist $\alpha_1, \alpha_2 \in \mathbb{N}$ with

$$\left(q^{r-1} - i + j - 1\right)(a+1) - jq^{r-1} = \alpha_1 (a+1) + \alpha_2 q^{r-1}$$

where $1 \leq j \leq i \leq a-s$, $(s-1)(q-1) \leq i-j < s(q-1)$, and $1 \leq s \leq a+1-q^{r-1}$. Then

$$\left(q^{r-1} - i + j - 1 - \alpha_1\right)(a+1) = (\alpha_2 + j)\, q^{r-1},$$

and, thus, $q^{r-1} - i + j - 1 - \alpha_1 \geq 0$. This leads to a contradiction since $q^{r-1} - i + j - 1 - \alpha_1$ is not a multiple of q^{r-1}. Consequently, each such integer $\left(q^{r-1} - i + j - 1\right)(a+1) - jq^{r-1}$ is an element of the gap set of P_∞. We apply a counting argument to see that each element of $G(P_\infty)$ is of the form $\left(q^{r-1} - i + j - 1\right)(a+1) - jq^{r-1}$ with $1 \leq j \leq i \leq a-s$, $(s-1)(q-1) \leq i-j < s(q-1)$, and $1 \leq s \leq a+1-q^{r-1}$; that is, we give a counting argument to show that there are precisely g integers of the form $\left(q^{r-1} - i + j - 1\right)(a+1) - jq^{r-1}$ with $1 \leq j \leq i \leq a-s$, $(s-1)(q-1) \leq i-j < s(q-1)$, and $1 \leq s \leq a+1-q^{r-1}$. It is not hard to see that

$$\left(q^{r-1} - i + j - 1\right)(a+1) - jq^{r-1} = \left(q^{r-1} - i' + j' - 1\right)(a+1) - j'q^{r-1}$$

where $1 \leq j \leq i \leq a-1$ and $1 \leq j' \leq i' \leq a-1$ implies

$$i = i' \text{ and } j = j'.$$

Hence, the number of such integers $\left(q^{r-1} - i + j - 1\right)(a+1) - jq^{r-1}$ is equal to the number of pairs (i,j) satisfying $1 \leq j \leq i \leq a-1$ and $i - j < q^{r-1} - 1$. Now, the number of (i,j) pairs with $1 \leq j \leq i \leq a-1$ and $i-j < q^{r-1}-1$ is

$$\sum_{i=1}^{a-1} \sum_{j=1}^{i} 1 - \sum_{i=q^{r-1}}^{a-1} \sum_{j=1}^{i-q^{r-1}+1} 1 = \frac{a\left(q^{r-1}-1\right)}{2},$$

which is the genus of the curve. This completes the proof that $G(P_\infty)$ is as claimed.

Next, we claim that the gap set of the point P_{00} (and of the point P_{0b}) is

$$G(P_{00}) = G(P_{0b}) = \left\{ (i-j)(a+1) + j : \begin{array}{c} 1 \leq j \leq i \leq a-s \text{ and} \\ (s-1)(q-1) \leq i-j < s(q-1) \\ \text{where } 1 \leq s \leq a+1-q^{r-1} \end{array} \right\}.$$

To see this, it is helpful to visualize the elements of the semigroup $H(P_{00})$ placed in an array as follows. Arrange the positive elements of $H(P_{00})$ in an array so that each row consists of consecutive integers. Consider $\alpha = (i-j)(a+1) + j$ where $1 \leq j \leq i \leq a-s$, $(s-1)(q-1) \leq i-j < s(q-1)$, and $1 \leq s \leq a+1-q^{r-1}$. Write $i - j = (s-1)(q-1) + k$ where $0 \leq k \leq q-2$. Then

$$\alpha = ((s-1)q - (s-2))\, a + (k-1)\, a + i.$$

Hence, if $\alpha \in H(P_{00})$, then α would be on row $(s-1)(q-1)+k$ of the array. However, the largest number on this row is

$$((s-1)(q-1)+k)\,a+(s-1)(q-1)+k,$$

and $\alpha > ((s-1)(q-1)+k)\,a+(s-1)(q-1)+k$ as $i > (s-1)\,q-(s-2)+k+1$. As a result, $\alpha \in G(P_{00})$. The claim now follows by the same counting argument applied above, because there are g positive integers of the form $(i-j)(a+1)+j$ with $1 \le j \le i \le a-s$, $(s-1)(q-1) \le i-j < s(q-1)$, and $1 \le s \le a+1-q^{r-1}$.

We will use these explicit descriptions of elements of the gap sets in the next section to find the Weierstrass semigroup of the triple $(P_\infty, P_{00}, P_{0b})$.

4 Determination of the semigroup $H(P_\infty, P_{00}, P_{0b})$

In this section, we find the Weierstrass semigroup of the triple $(P_\infty, P_{00}, P_{0b})$ on the norm-trace curve over $\mathbb{F}_{q^r}$. In fact, we produce the minimal generating set for this Weierstrass semigroup. To do so, we rely heavily on the results of [15]. In particular, we will use that the minimal generating set of the pair (P_∞, P_{00}) of points on the norm-trace curve over $\mathbb{F}_{q^r}$ is

$$\Gamma(P_\infty, P_{00}) = \left\{ v_{ij} : \begin{array}{c} 1 \le j \le i \le a-s, \\ (s-1)(q-1) \le i-j \le s(q-1)-1 \\ \text{for some } 1 \le s \le a+1-q^{r-1} \end{array} \right\}$$

where

$$v_{ij} := \left((a+1)\left(q^{r-1}-i+j-1\right)-jq^{r-1}, (a+1)(i-j)+j\right)$$

as proved in [15]. It is not difficult to see that $\Gamma(P_\infty, P_{00}) = \Gamma(P_\infty, P_{0b})$.

Theorem 1. *The minimal generating set of the Weierstrass semigroup of the triple $(P_\infty, P_{00}, P_{0b})$ of $\mathbb{F}_{q^r}$-rational points on the norm-trace curve over $\mathbb{F}_{q^r}$ is*

$$\Gamma(P_\infty, P_{00}, P_{0b}) = \left\{ \gamma_{i,j,t} : \begin{array}{c} 1 \le t \le i-j, 1 \le j < i \le a-s, \\ (s-1)(q-1) \le i-j \le s(q-1)-1 \\ \textit{where } 1 \le s \le a+1-q^{r-1} \end{array} \right\}$$

where
$\gamma_{i,j,t} :=$

$$\left(\left(q^{r-1}-i+j-1\right)(a+1)-jq^{r-1}, (i-j-t)(a+1)+j, (t-1)(a+1)+j\right).$$

Proof. Set

$$S := \left\{ \gamma_{i,j,t} : \begin{array}{l} 1 \le t \le i-j, 1 \le j < i \le a-s, \\ (s-1)(q-1) \le i-j \le s(q-1)-1 \\ \text{where } 1 \le s \le a+1-q^{r-1} \end{array} \right\}$$

and $\Gamma := \Gamma(P_\infty, P_{00}, P_{0b})$. First, we will show that $S \subseteq \Gamma$. Assume

$$s := \gamma_{i,j,t} \in S.$$

Then $s \in H(P_\infty, P_{00}, P_{0b})$ since

$$\left(\frac{x^{a+1-j}}{y^{i-j-t+1}(y-b)^t}\right)_\infty = s_1 P_\infty + s_2 P_{00} + s_3 P_{0b}.$$

Hence, $s \in P := \{p \in H(P_\infty, P_{00}, P_{0b}) : p_1 = s_1\}$ and so $P \neq \emptyset$. To conclude that $s \in \Gamma$, we will prove that s is minimal in P.

Suppose not; that is, suppose there exists $v \in P$ with $v \preceq s$ and $v \neq s$. Let $f \in \mathbb{F}_{q^r}(X)$ be so that

$$(f) = A - v_1 P_\infty - v_2 P_{00} - v_3 P_{0b}$$

where $A \geq 0$.

Suppose $v_2 < s_2$. Then $v_2 = s_2 - k$ with $k \in \mathbb{Z}^+$ and so

$$v_2 = (a+1)(i-j-t) + j - k.$$

If $j \leq k$, then

$$\left(f y^{i-j-t}\right)_\infty = (v_1 + (a+1)(i-j-t)) P_\infty + v_3 P_{0b}.$$

Hence,

$$w := \left((a+1)\left(q^{r-1} - t - 1\right) - j q^{r-1}, v_3\right) \in H(P_\infty, P_{0b}).$$

However,

$$\left((a+1)\left(q^{r-1} - t - 1\right) - j q^{r-1}, (a+1)t + j\right) \in \Gamma(P_\infty, P_{0b}),$$

$$w \preceq \left((a+1)\left(q^{r-1} - t - 1\right) - j q^{r-1}, (a+1)t + j\right),$$

and

$$w \neq \left((a+1)\left(q^{r-1} - t - 1\right) - j q^{r-1}, (a+1)t + j\right).$$

Consequently, it must be that $j > k$. Now,

$$\left(f y^{i-j-t} x^{j-k}\right)_\infty =$$

$$\left(v_1 + (a+1)(i-j-t) + (j-k) q^{r-1}\right) P_\infty + (v_3 - (j-k)) P_{0b}$$

which implies

$$w' := \left(v_1 + (a+1)(i-j-t) + (j-k) q^{r-1}, v_3 - (j-k)\right) \in H(P_\infty, P_{0b}).$$

This yields a contradiction since

$$w' \preceq \left((a+1)\left(q^{r-1} - t - 1\right) - k q^{r-1}, (a+1)t + k\right),$$

$$w' \neq \left((a+1)\left(q^{r-1}-t-1\right)-kq^{r-1},(a+1)t+k\right),$$

and

$$\left((a+1)\left(q^{r-1}-t-1\right)-kq^{r-1},(a+1)t+k\right) \in \Gamma\left(P_\infty,P_{0b}\right).$$

As a result, $v_2 = s_2$ and $v_3 < s_3$.

Write $v_3 = s_3 - k$ with $k \in \mathbb{Z}^+$ so that $v_3 = (a+1)(t-1)+j-k$. If $j \leq k$, then considering $\left(f(y-b)^{t-1}\right)$ leads to a contradiction as

$$\left((a+1)\left(q^{r-1}-i+t+j-2\right)-jq^{r-1},(a+1)(i-j-t)+j\right) \in H\left(P_\infty,P_{00}\right),$$

$$\left((a+1)\left(q^{r-1}-i+t+j-2\right)-jq^{r-1},(a+1)(i-j-t)+j\right) \preceq w,$$

$$\left((a+1)\left(q^{r-1}-i+t+j-2\right)-jq^{r-1},(a+1)(i-j-t)+j\right) \neq w,$$

and $w \in \Gamma\left(P_\infty,P_{00}\right)$ where

$$w := \left((a+1)\left(q^{r-1}-(i-t)+j-1\right)-jq^{r-1},(a+1)((i-t)-j)+j\right).$$

Thus, $j > k$. However, considering

$$\left(\frac{f(y-b)^{t-1}x^{j-k}}{y^{j-k+t}}\right)_\infty$$

gives

$$\left((a+1)\left(q^{r-1}-i+k-2\right)-kq^{r-1},(a+1)(i-k)+k\right) \in H\left(P_\infty,P_{00}\right).$$

Once again, this leads to a contradiction since

$$\left((a+1)\left(q^{r-1}-i+k-2\right)-kq^{r-1},(a+1)(i-k)+k\right) \preceq w',$$

$$\left((a+1)\left(q^{r-1}-i+k-2\right)-kq^{r-1},(a+1)(i-k)+k\right) \neq w',$$

and $w' \in \Gamma\left(P_\infty,P_{0b}\right)$ by [15] where

$$w' := \left((a+1)\left(q^{r-1}-i+k-1\right)-kq^{r-1},(a+1)(i-k)+k\right).$$

It follows that s is minimal in P and so $S \subseteq \Gamma$.

Next, we will show that $\Gamma \subseteq S$. Suppose $n \in \Gamma$. According to Lemma 1,

$$n \in G\left(P_\infty\right) \times G\left(P_{00}\right) \times G\left(P_{0b}\right).$$

Hence,

$$\begin{aligned} n_1 &= (a+1)\left(q^{r-1}-i_1+j_1-1\right)-j_1q^{r-1}, \\ n_2 &= (a+1)(i_2-j_2)+j_2, \text{ and} \\ n_3 &= (a+1)(i_3-j_3)+j_3 \end{aligned}$$

where $1 \leq j_k \leq i_k \leq a - s_k$ and $(s_k-1)(q-1) \leq i_k - j_k \leq s_k(q-1)-1$ for $k = 1,2,3$, with $1 \leq s_k \leq a+1-q^{r-1}$. We may assume, without loss of generality, that $j_2 \leq j_3$. Let $f \in \mathbb{F}_{q^r}(X)$ be so that $(f) = A - n_1 P_\infty - n_2 P_{00} - n_3 P_{0b}$ for some $A \geq 0$. Then

$$\begin{aligned}\left(f\left(y-b\right)^{i_3-j_3+1}\right) = {} & A + \left(\left(a+1\right)\left(i_3-j_3+1\right)-n_3\right)P_{0b} \\ & -\left(n_1+\left(a+1\right)\left(i_3-j_3+1\right)\right)P_\infty \\ & -n_2 P_{00}.\end{aligned}$$

Thus,

$$\left(n_1+\left(a+1\right)\left(i_3-j_3+1\right), n_2\right) \in H\left(P_\infty, P_{00}\right).$$

Consequently, there exists $u \in \Gamma\left(P_\infty, P_{00}\right)$ with

$$u \preceq \left(n_1+\left(a+1\right)\left(i_3-j_3+1\right), n_2\right)$$

and $u_2 = n_2$. According to [15], $u_1 = (a+1)\left(q^{r-1}-i_2+j_2-1\right) - j_2 q^{r-1}$. Notice that $n_1 < u_1$ since otherwise $(u_1, u_2, 0) \preceq n$, contradicting the minimality of n in $\{p \in H\left(P_\infty, P_{00}, P_{0b}\right) : p_2 = n_2\}$. As a result,

$$n_1 < u_1 \leq n_1 + \left(a+1\right)\left(i_3-j_3+1\right).$$

Set

$$h = \frac{\prod_{\beta\in\mathcal{B}}\left(y-\beta\right)}{y^{i_2-j_2}x^{j_2}\left(y-b\right)^{i_3-j_3}}$$

where $\mathcal{B} = \left\{\beta \in \mathbb{F}_{q^r} : Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\beta) = 0,\ \beta \neq 0, b\right\}$. Then

$$\begin{aligned}(h) = {} & \textstyle\sum_{\beta\neq 0,b}\left(a+1-j_2\right)P_{0\beta} - \left(u_1 - \left(a+1\right)\left(i_3-j_3+1\right)\right)P_\infty \\ & -\left(\left(a+1\right)\left(i_2-j_2\right)+j_2\right)P_{00} - \left(\left(a+1\right)\left(i_3-j_3\right)+j_2\right)P_{0b}.\end{aligned}$$

Thus, $w := \left(w_1, \left(a+1\right)\left(i_2-j_2\right)+j_2, \left(a+1\right)\left(i_3-j_3\right)+j_2\right) \in H\left(P_\infty, P_{00}, P_{0b}\right)$ where

$$w_1 = \max\left\{0, u_1 - \left(a+1\right)\left(i_3-j_3+1\right)\right\}.$$

However, $w \preceq n$ since $j_2 \leq j_3$. It follows that $w = n$; otherwise n is not minimal in $\{p \in H\left(P_\infty, P_{00}, P_{0b}\right) : p_2 = n_2\}$. Since $n_1 > 0$, we must have that

$$u_1 > \left(a+1\right)\left(i_3-j_3+1\right)$$

and $j_2 = j_3$. In particular,

$$\begin{aligned}n_1 &= \left(a+1\right)\left(q^{r-1}-\left(i_2+i_3-j_3+1\right)+j_2\right) \\ n_2 &= \left(a+1\right)\left(i_2-j_2\right)+j_2 \\ n_3 &= \left(a+1\right)\left(i_3-j_3\right)+j_2.\end{aligned}$$

It can be checked that $1 \leq i_2+i_3-j_3+1 \leq a-1$, from which it follows that $i_2+i_3-j_3+1 = i_1$ and $j_2 = j_1$. As a result,

$$n = \gamma_{i_2+i_3-j_3+1, j_2, i_3-j_3+1}$$

and so $n \in S$. Thus, $\Gamma \subseteq S$. This concludes the proof that $\Gamma\left(P_\infty, P_{00}, P_{0b}\right) = S$.

Example 1. Consider the norm-trace curve X defined by $y^9 + y^3 + y = x^{12}$ over $\mathbb{F}_{27}$. Notice that X has genus 48, the gap set of the point P_∞ is

$$\begin{aligned} G(P_\infty) &= \mathbb{N} \setminus \langle 9, 13 \rangle \\ &= \left\{ \begin{array}{l} 1,2,3,4,5,6,7,8,10,11,12,14,15,16,17,19,20,21,23,24,25,28, \\ 29,30,32,33,34,37,38,41,42,43,46,47,50,51,55,56,59,60,64, \\ 68,69,73,77,82,86,95 \end{array} \right\}, \end{aligned}$$

and the gap set of the points P_{00} and P_{0b} is

$$\begin{aligned} G(P_{00}) = G(P_{0b}) &= \mathbb{N} \setminus \langle 12, 13, 35, 58, 81 \rangle \\ &= \left\{ \begin{array}{l} 1,2,3,4,5,6,7,8,9,10,11,14,15,16,17,18,19,20,21,22,23,27, \\ 28,29,30,31,32,33,34,40,41,42,43,44,45,46,53,54,55,56,57, \\ 66,67,68,69,79,80,92 \end{array} \right\}. \end{aligned}$$

In [15], it is shown that

$\Gamma(P_\infty, P_{00}) =$

$$\left\{ \begin{array}{l} (1,23),(2,46),(3,69),(4,92),(5,11),(6,34),(7,57),(8,80),(10,22), \\ (11,45),(12,68),(14,10),(15,33),(16,56),(17,79),(19,21),(20,44), \\ (21,67),(23,9),(24,32),(25,55),(28,20),(29,43),(30,66),(32,8),(33,31), \\ (34,54),(37,19),(38,42),(41,7),(42,30),(43,53),(46,18),(47,41),(50,6), \\ (51,29),(55,17),(56,40),(59,5),(60,28),(64,16),(68,4),(69,27), \\ (73,15),(77,3),(82,14),(86,2),(95,1) \end{array} \right\}.$$

According to Theorem 1, the minimal generating set of the Weierstrass semigroup of the triple $(P_\infty, P_{00}, P_{0b})$ is

$\Gamma\left(P_{\infty}, P_{00}, P_{0b}\right) =$

$$\left\{\begin{array}{l}(1,10,10),(2,7,33),(2,20,20),(2,33,7),(3,4,56),\\(3,17,43),(3,30,30),(3,43,17),(3,56,4),(4,1,79),\\(4,14,66),(4,27,53),(4,40,40),(4,53,27),(4,66,14),\\(4,79,1),(6,8,21),(6,21,8)(7,5,44),(7,18,31),\\(7,31,18),(7,44,5),(8,2,67),(8,15,54),(8,28,41),\\(8,41,28),(8,54,15),(8,67,2),(10,9,9),(11,6,32),\\(11,19,19),(11,32,6),(12,3,55),(12,16,42),(12,29,29),\\(12,42,16),(12,55,3),(15,7,20),(15,20,7),(16,4,43),\\(16,17,30),(16,30,17),(16,43,4),(17,1,66),(17,14,53),\\(17,27,40),(17,40,27),(17,53,14),(17,66,1),(19,8,8),\\(20,5,31),(20,18,18),(20,31,5),(21,2,54),(21,15,41),\\(21,28,28),(21,41,15),(21,54,2),(24,6,19),(24,19,6),\\(25,3,42),(25,16,29),(25,29,16),(25,42,3),(28,7,7),\\(29,4,30),(29,17,17),(29,30,4),(30,1,53),(30,14,40),\\(30,27,27),(30,40,14),(30,53,1),(33,5,18),(33,18,5),\\(34,2,41),(34,15,28),(34,28,15),(34,41,2),(37,6,6),\\(38,3,29),(38,16,16),(38,29,3),(42,4,17),(42,17,4),\\(43,1,40),(43,14,27),(43,27,14),(43,40,1),(46,5,5),\\(47,2,28),(47,15,15),(47,28,2),(51,3,16),(51,16,3),\\(55,4,4),(56,1,27),(56,14,14),(56,27,1),(60,2,15),\\(60,15,2),(64,3,3),(69,1,14),(69,14,1),(73,2,2),\\(82,1,1)\end{array}\right\}.$$

Acknowledgements. The referee's comments and corrections are greatly appreciated.

References

1. Arbarello, E., Cornalba, M., Griffiths, P., Harris, J.: *Geometry of Algebraic Curves*, Springer-Verlag, 1985
2. Ballico, E., Kim, S. J.: Weierstrass multiple loci of n-pointed algebraic curves. J. Algebra **199** (1998), no. 2, 455–471
3. Carvalho, C., Kato, T.: On Weierstrass semigroups and sets: a review of new results, Geom. Dedicata, to appear
4. Carvalho, C., Torres, F.: On Goppa codes and Weierstrass gaps at several points. Des. Codes Cryptogr. **35** (2005), no. 2, 211–225
5. Garca, A., Kim, S. J., Lax, R. F.: Consecutive Weierstrass gaps and minimum distance of Goppa codes. J. Pure Appl. Algebra **84** (1993), no. 2, 199–207
6. Geil, O.: On codes from norm-trace curves. Finite Fields Appl. **9** (2003), no. 3, 351–371
7. Homma, M., Kim, S. J.: Goppa codes with Weierstrass pairs. J. Pure Appl. Algebra **162** (2001), no. 2-3, 273–290
8. Ishii, N.: A certain graph obtained from a set of several points on a Riemann surface. Tsukuba J. Math. **23** (1999), no. 1, 55–89

9. Kim, S. J.: On the index of the Weierstrass semigroup of a pair of points on a curve. Arch. Math. (Basel) **62** (1994), no. 1, 73–82
10. Matthews, G. L.: Codes from the Suzuki function field. IEEE Trans. Inform. Theory **50** (2004), no. 12, 3298–3302
11. Matthews, G. L.: Some computational tools for estimating the parameters of algebraic geometry codes. Coding theory and quantum computing, 19–26, Contemp. Math., **381**, Amer. Math. Soc., Providence, RI, 2005
12. Matthews, G. L.: Weierstrass semigroups and codes from a quotient of the Hermitian curve. Des. Codes Cryptogr. **37** (2005), no. 3, 473–492
13. Matthews, G. L.: The Weierstrass semigroup of an m-tuple of collinear points on a Hermitian curve. Finite fields and applications, 12–24, Lecture Notes in Comput. Sci., **2948**, Springer, Berlin, 2004
14. Matthews, G. L.: Weierstrass pairs and minimum distance of Goppa codes. Des. Codes Cryptogr. **22** (2001), no. 2, 107–121
15. Munuera, C., Tizziotti, G. C., Torres, F.: Two-point codes on Norm-Trace curves. Coding Theory and Applications, Second International Castle Meeting, ICMCTA 2008 (A. Barbero Ed.), 128-136, Lecture Notes in Comput. Sci. **5228**, Springer-Verlag Berlin Heidelberg 2008