The Weierstrass semigroup of an m-tuple of collinear points on a Hermitian curve

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. We examine the structure of the Weierstrass semigroup of an m-tuple of points on a smooth, projective, absolutely irreducible curve X over a finite field $\mathbb{F}$. A criteria is given for determining a minimal subset of semigroup elements which generate such a semigroup where $2 \leq m \leq \mid \mathbb{F} \mid$. For all $2 \leq m \leq q+1$, we determine the Weierstrass semigroup of any m-tuple of collinear $\mathbb{F}_{q^2}$-rational points on a Hermitian curve $y^q + y = x^{q+1}$.

1 Introduction

Let X be a smooth, projective, absolutely irreducible curve of genus $g > 1$ over a finite field $\mathbb{F}$. Let $\mathbb{F}(X)$ denote the field of rational functions on X defined over $\mathbb{F}$. The divisor of a rational function $f \in \mathbb{F}(X)$ will be denoted by (f) and the divisor of poles of f will be denoted by $(f)_\infty$.

Given m distinct $\mathbb{F}$-rational points $P_1, \ldots, P_m$ on X, the Weierstrass semigroup $H(P_1, \ldots, P_m)$ of the m-tuple $(P_1, \ldots, P_m)$ is defined by

$$H(P_1, \ldots, P_m) = \left\{ (\alpha_1, \ldots, \alpha_m) \in \mathbb{N}_0^m : \exists f \in \mathbb{F}(X) \text{ with } (f)_\infty = \sum_{i=1}^{m} \alpha_i P_i \right\},$$

and the Weierstrass gap set $G(P_1, \ldots, P_m)$ of the m-tuple $(P_1, \ldots, P_m)$ is defined by

$$G(P_1, \ldots, P_m) = \mathbb{N}_0^m \setminus H(P_1, \ldots P_m),$$

where $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ denotes the set of nonnegative integers. If $m = 1$, the Weierstrass gap set is the classically studied gap sequence. In [1], the authors generalized the notion of the semigroup of a point to the semigroup of a pair of points on a curve. This study was carried on by S. J. Kim [7] and M. Homma [5]. The Weierstrass gap set of an m-tuple of points where $m \geq 2$ has been examined by E. Ballico and Kim [2], and more recently, by C. Carvalho and F. Torres [3]. Weierstrass gap sets play an interesting role in the construction and analysis of algebraic geometry codes (see [4], [9], [6], [3]). While $\mid G(P_1) \mid = g$ for any $\mathbb{F}$-rational point P_1 on X, the cardinality of the set $G(P_1, \ldots, P_m)$ where $m \geq 2$ depends on the choice of points $P_1, \ldots, P_m$ [1]. However, any pair of $\mathbb{F}_{q^2}$-rational points on a Hermitian curve $y^q + y = x^{q+1}$ has the same Weierstrass semigroup [9]. The analogous result does not hold for triples of $\mathbb{F}_{q^2}$-rational points on a Hermitian curve [10].

In this paper, we consider the notion of a minimal generating subset of a Weierstrass semigroup of an m-tuple of points on an arbitrary (smooth, projective, absolutely irreducible) curve over a finite field $\mathbb{F}$. In Section 2, we discuss properties of minimal elements of the Weierstrass semigroup. This section concludes with a useful characterization of the elements of the minimal generating set of the Weierstrass semigroup of an m-tuple of points for $2 \leq m \leq |\mathbb{F}|$. An interesting application of this is found in Section 3 where we see that any m-tuple of collinear $\mathbb{F}_{q^2}$-rational points on a Hermitian curve $y^q + y = x^{q+1}$ has the same Weierstrass semigroup. In addition, we determine this Weierstrass semigroup and its minimal generating set.

2 Results for arbitrary curves

Let X be a smooth, projective, absolutely irreducible curve of genus $g > 1$ over a finite field $\mathbb{F}$. Fix m distinct $\mathbb{F}$-rational points $P_1, \dots, P_m$ on X, where $2 \leq m \leq |\mathbb{F}|$. For $1 \leq l \leq m$, set $H_l := H(P_1, \dots, P_l)$. Define a partial order $\preceq$ on $\mathbb{N}_0^m$ by $(n_1, \dots, n_m) \preceq (p_1, \dots, p_m)$ if and only if $n_i \leq p_i$ for all i, $1 \leq i \leq m$. It is convenient to collect here two results from [3] that will be used in this section.

Lemma 1. *[3] If $(n_1, \dots, n_m), (p_1, \dots, p_m) \in H_m$ and $n_j = p_j$ for some j, $1 \leq j \leq m$, then there exists $\mathbf{q} = (q_1, \dots, q_m) \in H_m$ whose coordinates satisfy the following properties:*

1. *$q_i = max(n_i, p_i)$ for $i \neq j$ and $n_i \neq p_i$.*
2. *$q_i \leq n_i$ for $i \neq j$ and $n_i = p_i$.*
3. *$q_j = n_j = 0$ or $q_j < n_j$.*

Lemma 2. *[3] Suppose that there exists i, $1 \leq i \leq m$, such that $(n_1, \dots, n_m)$ is a minimal element of the set $\{\mathbf{p} \in H_m : p_i = n_i\}$ with respect to $\preceq$. If $n_i > 0$ and $n_j > 0$ for some j, $1 \leq j \leq m$, $j \neq i$, then $n_i \in G(P_i)$.*

Proposition 3. *Let $\mathbf{n} \in \mathbb{N}^m$. Then $\mathbf{n}$ is minimal in $\{\mathbf{p} \in H_m : p_i = n_i\}$ with respect to $\preceq$ for some i, $1 \leq i \leq m$, if and only if $\mathbf{n}$ is minimal in the set $\{\mathbf{p} \in H_m : p_i = n_i\}$ with respect to $\preceq$ for all i, $1 \leq i \leq m$.*

Proof. Suppose $\mathbf{n} \in \mathbb{N}^m$ is minimal in $\{\mathbf{p} \in H_m : p_i = n_i\}$ with respect to $\preceq$ for some i, $1 \leq i \leq m$. Without loss of generality, we may assume that $i = 1$. Suppose there exists j, $2 \leq j \leq m$, such that $\mathbf{n}$ is not minimal in $\{\mathbf{p} \in H_m : p_j = n_j\}$. Then there exists $\mathbf{v} \in H_m$ such that $\mathbf{v} \preceq \mathbf{n}$, $\mathbf{v} \neq \mathbf{n}$, and $v_j = n_j$. Note that $v_1 < n_1$ as otherwise $\mathbf{v} \in \{\mathbf{p} \in H_m : p_1 = n_1\}$ contradicting the minimality of $\mathbf{n}$. Applying Lemma 1, we see that there exists $\mathbf{q} \in H_m$ with $q_1 = n_1$, $q_j < n_j$, and $q_i \leq n_i$ for all $1 \leq i \leq m$. Thus, $\mathbf{q} \preceq \mathbf{n}$, $\mathbf{q} \neq \mathbf{n}$, and $\mathbf{q} \in \{\mathbf{p} \in H_m : p_1 = n_1\}$. This contradicts the minimality of $\mathbf{n} \in \{\mathbf{p} \in H_m : p_1 = n_1\}$. Thus, $\mathbf{n}$ is minimal in $\{\mathbf{p} \in H_m : p_j = n_j\}$ for all j, $1 \leq j \leq m$.

Using these ideas, we set out to describe a subset of H_m that generates the entire semigroup H_m. To begin, set $\Gamma_1^+ = H(P_1)$, the Weierstrass semigroup of the point P_1. For $2 \leq l \leq m$, define

$$\Gamma_l^+ := \{\mathbf{n} \in \mathbb{N}^l : \mathbf{n} \text{ is minimal in } \{\mathbf{p} \in H_l : p_i = n_i\} \text{ for some } i, 1 \leq i \leq l\}.$$

The notion of Γ_2^+ is due to Kim [7]. As an immediate consequence of Proposition 3 and Lemma 2, we obtain the following result.

Lemma 4. *For $2 \leq l \leq m$, $\Gamma_l^+ \subseteq G(P_1) \times \cdots \times G(P_l)$.*

Using Γ_l^+, we will now describe a subset Γ_l of H_l for $1 \leq l \leq m$. First, set $\Gamma_1 = \Gamma_1^+ = H(P_1)$. For $2 \leq l \leq m$, define

$$\Gamma_l := \Gamma_l^+ \cup \left\{ \begin{array}{c} \mathbf{n} \in \mathbb{N}_0^l : (n_{i_1}, \ldots, n_{i_k}) \in \Gamma_k^+ \text{ for some } \{i_1, \ldots, i_m\} = \{1, \ldots, m\} \\ \text{such that } i_1 < \cdots < i_k \text{ and } n_{i_{k+1}} = \cdots = n_{i_m} = 0 \end{array} \right\}.$$

Clearly, Γ_m is completely determined by $\{\Gamma_l^+ : 1 \leq l \leq m\}$.

Example 5. Consider the curve defined by $y^8 + y = x^9$ over $\mathbb{F}_{64}$. Let $P_1 = P_\infty$ denote the point at infinity and $P_2 = P_{00}$ denote the common zero of x and y. It is well known that the Weierstrass gap set of the point P_1 (and P_2) is

$$\begin{array}{ccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 10 & 11 & 12 & 13 & 14 & 15 & \\ 19 & 20 & 21 & 22 & 23 & & \\ 28 & 29 & 30 & 31 & & & \\ 37 & 38 & 39 & & & & \\ 46 & 47 & & & & & \\ 55 & & & & & & \end{array} .$$

Equivalently, the Weierstrass semigroup of the point P_1 is the additive subsemigroup of $\mathbb{N}_0$ generated by 8 and 9; that is, $H(P_1) = \langle 8, 9 \rangle := \{8a+9b : a, b \in \mathbb{N}_0\}$. Hence, $\Gamma_1 = \langle 8, 9 \rangle$. According to [9],

$$\Gamma_2^+ = \left\{ \begin{array}{l} (1,55), (2,47), (3,39), (4,31), (5,23), (6,15), (7,7), (10,46), \\ (11,38), (12,30), (13,22), (14,14), (15,6), (19,37), (20,29), \\ (21,21), (22,13), (23,5), (28,28), (29,20), (30,12), (31,4), \\ (37,19), (38,11), (39,3), (46,10), (47,2), (55,1) \end{array} \right\}.$$

Then

$$\Gamma_2 = \Gamma_2^+ \cup \{(n,0), (0,n) : n \in \langle 8, 9 \rangle\}.$$

We will show that Γ_m generates H_m by taking least upper bounds. Given $\mathbf{u_1}, \ldots, \mathbf{u_l} \in \mathbb{N}_0^m$, define the least upper bound of $\mathbf{u_1}, \ldots, \mathbf{u_l}$ by

$$\text{lub}\{\mathbf{u_1}, \ldots, \mathbf{u_l}\} = (\max\{u_{1_1}, \ldots, u_{l_1}\}, \ldots, \max\{u_{1_m}, \ldots, u_{l_m}\}) \in \mathbb{N}_0^m$$

In [7], Kim proved that $H_2 = \{\text{lub}\{\mathbf{u_1}, \mathbf{u_2}\} \in \mathbb{N}_0^2 : \mathbf{u_1}, \mathbf{u_2} \in \Gamma_2\}$. To obtain a similar result for H_m where $m \geq 3$, we use the next fact which follows immediately from [3].

Proposition 6. *Suppose that* $1 \leq l \leq m \leq |\mathbb{F}|$ *and* $\mathbf{u_1}, \ldots, \mathbf{u_l} \in H_m$. *Then* $\mathrm{lub}\{\mathbf{u_1}, \ldots, \mathbf{u_l}\} \in H_m$.

Proof. Let $\mathbf{q_2} := \mathrm{lub}\{\mathbf{u_1}, \mathbf{u_2}\}$. For $3 \leq i \leq l$, define $\mathbf{q_i} := \mathrm{lub}\{\mathbf{q_{i-1}}, \mathbf{u_i}\}$. According to [3], $\mathbf{q_2} \in H_m$. Repeated application gives $\mathbf{q_i} \in H_m$ for all $i \in \{2, \ldots, l\}$. This completes the proof as $\mathrm{lub}\{\mathbf{u_1}, \ldots, \mathbf{u_l}\} = \mathbf{q_l} \in H_m$.

Theorem 7. *If* $1 \leq m \leq |\mathbb{F}|$, *then*

$$H_m = \{\mathrm{lub}\,\{\mathbf{u_1}, \ldots, \mathbf{u_m}\} \in \mathbb{N}_0^m : \mathbf{u_1}, \ldots, \mathbf{u_m} \in \Gamma_m\}.$$

Proof. The fact that $\{\mathrm{lub}\,\{\mathbf{u_1}, \ldots, \mathbf{u_m}\} \in \mathbb{N}_0^m : \mathbf{u_1}, \ldots, \mathbf{u_m} \in \Gamma_m\} \subseteq H_m$ follows from Proposition 6.

Suppose $\mathbf{n} \in H_m \setminus \Gamma_m$. Without loss of generality, we may assume that $\mathbf{n} \in \mathbb{N}^m$. (Otherwise, $(n_{i_1}, \ldots n_{i_l}) \in \mathbb{N}^l$ for some $\{i_1, \ldots, i_m\} = \{1, \ldots, m\}$ such that $i_1 < \cdots < i_l$ and $n_{i_{l+1}} = \cdots = n_{i_m} = 0$, and the same argument applies to $(n_{i_1}, \ldots n_{i_l})$). Then, according to Proposition 3, $\mathbf{n}$ is not minimal in $\{\mathbf{p} \in H_m : p_i = n_i\}$ for any i, $1 \leq i \leq m$. Hence, there exists $\mathbf{u_i} \in \Gamma_m$ with $u_{i_i} = n_i$, $\mathbf{u_i} \preceq \mathbf{n}$, and $\mathbf{u_i} \neq \mathbf{n}$ for each i, $1 \leq i \leq m$. Then $\mathbf{n} = \mathrm{lub}\{\mathbf{u_1}, \ldots, \mathbf{u_m}\}$, completing the proof.

According to Theorem 7 and the definition of Γ_m, the Weierstrass semigroup H_m is completely determined by $\{\Gamma_l^+ : 1 \leq l \leq m\}$. We conclude this section with a useful characterization of elements of the sets Γ_l^+, $1 \leq l \leq m$. To do this, it is helpful to consider dimensions of certain divisors. For a divisor D on X defined over $\mathbb{F}$, let $L(D)$ denote the set of rational functions $f \in \mathbb{F}(X)$ with divisor $(f) \geq -D$ together with the zero function. Then $L(D)$ is a finite dimensional vector space over $\mathbb{F}$. Let $l(D)$ denote the dimension of the vector space $L(D)$ over $\mathbb{F}$. The Riemann-Roch Theorem states that $l(D) = \deg\, D + 1 - g + l(K - D)$, where K is any canonical divisor on X. This gives a characterization of elements of the Weierstrass semigroup of an m-tuple $(P_1, \ldots, P_m)$ according to dimensions of divisors supported by the points $P_1, \ldots, P_m$. This is an easy generalization of a lemma due to Kim [7].

Lemma 8. *For* $(\alpha_1, \ldots, \alpha_m) \in \mathbb{N}^m$, *the following are equivalent:*
(i) $(\alpha_1, \ldots, \alpha_m) \in H(P_1, \ldots, P_m)$.
(ii) $l(\sum_{i=1}^m \alpha_i P_i) = l((\alpha_j - 1)P_j + \sum_{i=1, i \neq j}^m \alpha_i P_i) + 1$ *for all* j, $1 \leq j \leq m$.

Proposition 9. *Let* $1 \leq l \leq m \leq |\ \mathbb{F}\ |$ *and* $\mathbf{n} \in \mathbb{N}^l$. *Then* $\mathbf{n} \in \Gamma_l^+$ *if and only if* $\mathbf{n} \in H_l$ *and* $l(\sum_{j=1}^l (n_j - 1)P_j) = l((n_k - 1)P_k + \sum_{j=1, j \neq k}^l n_j P_j)$ *for all* k, $1 \leq k \leq l$.

Proof. Suppose $\mathbf{n} \in \Gamma_l^+$. If $l(\sum_{j=1}^l (n_j - 1)P_j) \neq l((n_k - 1)P_k + \sum_{j=1, j \neq k}^l n_j P_j)$ for some k, $1 \leq k \leq l$, then there exists $\mathbf{v} \in H_l$ with $\mathbf{v} \preceq \mathbf{n}$, $v_k \leq n_k - 1$, and $v_t = n_t$ for some t, $1 \leq t \leq l$. This contradicts the assumption that $\mathbf{n}$ is minimal in $\{\mathbf{p} \in H_l : p_t = n_t\}$. Thus, $l(\sum_{j=1}^l (n_j - 1)P_j) = l((n_k - 1)P_k + \sum_{j=1, j \neq k}^l n_j P_j)$ for all k, $1 \leq k \leq l$.

Suppose $\mathbf{n} \in H_l$ and $l(\sum_{j=1}^{l}(n_j-1)P_j) = l((n_k-1)P_k + \sum_{j=1, j\neq k}^{l} n_jP_j)$ for all k, $1 \leq k \leq l$. This implies

$$L\left((n_1-1)P_1 + \sum_{j=2}^{l} n_jP_j\right) = L\left(\sum_{j=1}^{l}(n_j-1)P_j\right) = L\left((n_k-1)P_k + \sum_{\substack{j=1 \\ j\neq k}}^{l} n_jP_j\right)$$

for all k, $1 \leq k \leq l$, as $L(\sum_{j=1}^{l}(n_j-1)P_j) \subseteq L((n_k-1)P_k + \sum_{j=1,j\neq k}^{l} n_jP_j)$. If $\mathbf{n} \notin \Gamma_l^+$, then there exists $\mathbf{u} \in H_l$ with $u_1 = n_1$, $\mathbf{u} \preceq \mathbf{n}$, and $\mathbf{u} \neq \mathbf{n}$. In particular, $u_k < n_k$ for some k, $2 \leq k \leq l$. Thus, there exists a rational function $f \in L((n_k-1)P_k + \sum_{j=1,j\neq k}^{l} n_jP_j)$ such that $f \notin L((n_1-1)P_1 + \sum_{j=2}^{l} n_jP_j)$, which is a contradiction.

3 Computation of $H(P_1, \ldots, P_m)$ for collinear points $P_1, \ldots, P_m$ on a Hermitian curve

In this section, we restrict our attention to the curve X defined by $y^q + y = x^{q+1}$ over $\mathbb{F}_{q^2}$. Given $a, b \in \mathbb{F}_{q^2}$ with $b^q + b = a^{q+1}$, let P_{ab} denote the common zero of $x-a$ and $y-b$. Fix $a \in \mathbb{F}_{q^2}$. Then there are exactly q elements $b_2, \ldots, b_{q+1} \in \mathbb{F}_{q^2}$ such that $b_i^q + b_i = a^{q+1}$. Set $P_1 = P_\infty, P_2 = P_{ab_2}, P_3 = P_{ab_3}, \ldots, P_{q+1} = P_{ab_{q+1}}$. For $1 \leq m \leq q+1$, let $H_m := H(P_1, \ldots, P_m)$. We set out to determine Γ_m for all $1 \leq m \leq q+1$.

Notice that the divisors of $x-a$ and y are given by

$$(x-a) = \sum_{i=2}^{q+1} P_{ab_i} - qP_\infty \qquad \text{and} \qquad (y) = (q+1)(P_{00} - P_\infty).$$

It will also be useful to consider functions $h_{ab_i} := y - b_i - a^q(x-a)$ where $2 \leq i \leq q+1$. Note that the divisor of h_{ab_i} is given by

$$(h_{ab_i}) = (q+1)(P_{ab_i} - P_\infty)$$

(see [8]). Using the functions x and y and the fact that X is a curve of genus $\frac{q(q-1)}{2}$, one can check $H(P_1) = \langle q, q+1 \rangle$ and that the Weierstrass gap set $G(P_1)$ is

$$\begin{array}{ccccc} 1 & 2 & \cdots & q-2 & q-1 \\ (q+1)+1 & (q+1)+2 & \cdots & (q+1)+(q-2) & \\ \vdots & \vdots & \iddots & & \\ (q-3)(q+1)+1 & (q-3)(q+1)+2 & & & \\ (q-2)(q+1)+1 & & & & \end{array} .$$

In fact, the above set is the Weierstrass gap set of any $\mathbb{F}_{q^2}$-rational point on X. Given $\alpha \in G(P)$ where P is any $\mathbb{F}_{q^2}$-rational point, α can be written uniquely as $\alpha = (t-j)(q+1)+j$ with $1 \le j \le t \le q-1$. Here, j denotes the column containing α and t denotes the diagonal containing α in the above diagram.

From above, $\Gamma_1^+ = H(P_1) = \langle q, q+1 \rangle$. According to [9, Theorem 3.7],

$$\Gamma_2^+ = \left\{ ((t_1-j)(q+1)+j, (t_2-j)(q+1)+j) : \begin{array}{l} 1 \le j \le t_1, t_2 \le q-1, \\ t_1+t_2 = q+j-1 \end{array} \right\}.$$

To describe Γ_m^+ for $3 \le m \le q+1$, we must set up some notation. Given $1 \le m \le q+1$, $\mathbf{t} = (t_1, \dots, t_m) \in \mathbb{N}^m$, and $j \in \mathbb{N}$, define

$$\boldsymbol{\gamma}_{\mathbf{t},j} := ((t_1-j)(q+1)+j, (t_2-j)(q+1)+j, \dots, (t_m-j)(q+1)+j) \in \mathbb{N}_0^m.$$

Notice that if $1 \le j \le t_i \le q-1$ for all $1 \le i \le m$, then

$$\boldsymbol{\gamma}_{\mathbf{t},j} \in G(P_1) \times G(P_2) \times \cdots \times G(P_m).$$

We next show that certain $\boldsymbol{\gamma}_{\mathbf{t},j}$ form a generating set for the Weierstrass semigroup H_m.

Theorem 10. *Let $a \in \mathbb{F}_{q^2}$ and $P_1 = P_\infty, P_2 = P_{ab_2}, P_3 = P_{ab_3}, \dots, P_{q+1} = P_{ab_{q+1}}$ be $q+1$ distinct $\mathbb{F}_{q^2}$-rational points on the Hermitian curve X defined by $y^q + y = x^{q+1}$. For $2 \le m \le q+1$,*

$$\Gamma_m^+ = \left\{ \boldsymbol{\gamma}_{\mathbf{t},j} : \begin{array}{l} \sum_{i=1}^m t_i = q + (m-1)(j-1), \\ 1 \le j \le t_i \le q-1 \text{ for all } 1 \le i \le m \end{array} \right\}.$$

In particular, the Weierstrass semigroup $H(P_1, \dots, P_m)$ is generated by

$$\left\{ \begin{array}{c} \mathbf{n} \in \mathbb{N}_0^m : (n_{i_1}, \dots n_{i_l}) = \boldsymbol{\gamma}_{\mathbf{t},j} \in \Gamma_l^+ \text{ and } n_{i_{l+1}} = \cdots = n_{i_m} = 0 \\ \text{for some } l \in \mathbb{N} \text{ and } \{i_1, \dots, i_m\} = \{1, \dots, m\} \end{array} \right\}.$$

Proof. We begin by setting up some notation. For $2 \le m \le q+1$, set

$$S_m := \left\{ \boldsymbol{\gamma}_{\mathbf{t},j} : \begin{array}{l} \sum_{i=1}^m t_i = q + (m-1)(j-1), \\ 1 \le j \le t_i \le q-1 \text{ for all } 1 \le i \le m \end{array} \right\}.$$

For each $2 \le i \le q+1$, let $h_i := h_{ab_i} \in \mathbb{F}_{q^2}(X)$ be as above so that

$$(h_i) = (q+1)P_i - (q+1)P_1.$$

Given $\mathbf{v} := (v_1, \dots, v_m) \in \mathbb{Z}^m$, let $\mathbf{v}^+ := (v_{i_1}, \dots, v_{i_l}) \in \mathbb{N}^l$ where $i_1 < \cdots < i_l$ and $v_i > 0$ if and only if $i = i_r$ for some $1 \le r \le l$; that is, $\mathbf{v}^+$ is the vector formed from $\mathbf{v}$ by deleting each coordinate of $\mathbf{v}$ containing a negative or zero entry.

We will prove that $\Gamma_m^+ = S_m$ by induction on m. By [9, Theorem 3.7],

$$\Gamma_2^+ = \{ \boldsymbol{\gamma}_{(t_1,t_2),j} : t_1 + t_2 = q+j-1, 1 \le j \le t_1, t_2 \le q-1 \} = S_2,$$

which settles the case where $m = 2$. We now proceed by induction on $m \ge 3$. Assume that $\Gamma_l^+ = S_l$ holds for all $2 \le l \le m-1$.

First, we claim that $S_m \subseteq \Gamma_m^+$. Let $\boldsymbol{\gamma}_{\mathbf{t},j} \in S_m$. Then

$$\left(\frac{(x-a)^{q-j+1}}{h_2^{t_2-j+1} h_3^{t_3-j+1} \cdots h_m^{t_m-j+1}}\right)_\infty = \sum_{i=1}^{m} ((t_i - j)(q+1) + j) P_i.$$

Hence, $\boldsymbol{\gamma}_{\mathbf{t},j} \in H_m$.

In order to show that $\boldsymbol{\gamma}_{\mathbf{t},j} \in \Gamma_m^+$, it suffices to prove that $\boldsymbol{\gamma}_{\mathbf{t},j}$ is minimal in $\{\mathbf{p} \in H_m : p_1 = (t_1 - j)(q+1) + j\}$. Suppose $\boldsymbol{\gamma}_{\mathbf{t},j}$ is not minimal in

$$\{\mathbf{p} \in H_m : p_1 = (t_1 - j)(q+1) + j\}.$$

Then there exists $\mathbf{u} \in H_m$ with $u_1 = (t_1 - j)(q+1) + j$, $\mathbf{u} \preceq \boldsymbol{\gamma}_{\mathbf{t},j}$, and $\mathbf{u} \neq \boldsymbol{\gamma}_{\mathbf{t},j}$. Let $f \in \mathbb{F}_{q^2}(X)$ be such that $(f)_\infty = u_1 P_1 + \cdots + u_m P_m$. Without loss of generality, we may assume that $u_m < (t_m - j)(q+1) + j$ as $\mathbf{u} \neq \boldsymbol{\gamma}_{\mathbf{t},j}$ gives $u_i < (t_i - j)(q+1) + j$ for some $2 \leq i \leq m$ and a similar argument holds if $2 \leq i \leq m-1$. Hence,

$$u_m = (t_m - j)(q+1) + j - k$$

for some $k \geq 1$. There are two cases to consider:

(1) $j > k$.
(2) $j \leq k$.

Case (1): Suppose $j > k$. Then

$$\left(f h_m^{t_m - j}(x-a)^{j-k}\right)_\infty = ((t_1 + t_m - j - k)(q+1) + k) P_1 + \sum_{i=2}^{m-1} \max\{u_i - (j-k), 0\} P_i.$$

Therefore,

$$\mathbf{v} := ((t_1 + t_m - j - k)(q+1) + k, v_2, \ldots, v_{m-1}) \in H_{m-1},$$

where $v_i = \max\{u_i - (j-k), 0\}$ for $2 \leq i \leq m-1$. Set

$$\mathbf{w} := \boldsymbol{\gamma}_{(t_1 + t_m - j, t_2 - j + 1 + k, t_3 - j + k, \ldots, t_{m-1} - j + k), k}.$$

Clearly,

$$\mathbf{v} \preceq \mathbf{w}.$$

Note that

$$\mathbf{w} \in S_{m-1}$$

since $t_1 + t_m - j + t_2 - j + 1 + k + \sum_{i=3}^{m-1}(t_i - j + k) = q + (m-2)(k-1)$, $k \leq t_2 - j + 1 + k \leq t_2 \leq q-1$ as $j - k > 0$, $k \leq t_i - j + k \leq t_i \leq q-1$ for $3 \leq i \leq m-1$, and $k \leq j \leq t_1 + t_m - j \leq q-1$ (otherwise, $\sum_{i=2}^{m-1} t_i \leq (m-2)(j-1) < (m-2)j$). By the induction hypothesis, $S_{m-1} = \Gamma_{m-1}^+$, and so

$$\mathbf{w} \in \Gamma_{m-1}^+.$$

By Proposition 3, $\mathbf{w}$ is minimal in $\{\mathbf{p} \in H_{m-1} : p_1 = (t_1+t_m-j-k)(q+1)+k\}$. This leads to a contradiction as

$$\begin{aligned}&\mathbf{v} \in \{\mathbf{p} \in H_{m-1} : p_1 = (t_1+t_m-j-k)(q+1)+k\},\\&\mathbf{v} \preceq \mathbf{w}, \text{ and}\\&\mathbf{v} \neq \mathbf{w}.\end{aligned}$$

Case (2): Suppose $j \leq k$. Then

$$\left(fh_m^{t_m-j}\right)_\infty = ((t_1+t_m-2j)(q+1)+j)P_1 + \sum_{i=2}^{m-1} u_i P_i$$

which implies that

$$\mathbf{v} := ((t_1+t_m-j-j)(q+1)+j, u_2, \ldots, u_{m-1}) \in H_{m-1}.$$

Note that there exists i, $2 \leq i \leq m-1$, such that $t_i < q-1$ since otherwise $2j \leq t_1+t_m = q+(m-1)(j-1)-(m-2)(q-1)$ implies that $0 \leq 2-m$ contradicting the assumption that $m \geq 3$. We may assume that $i=2$ as a similar argument holds in the case $2 < i \leq m-1$. Set

$$\mathbf{w} := \gamma_{(t_1+t_m-j, t_2+1, t_3 \ldots, t_{m-1}), j}.$$

Clearly,

$$\mathbf{v} \preceq \mathbf{w}.$$

Also note that

$$\mathbf{w} \in S_{m-1}$$

since $t_1+t_m-j+t_2+1+\sum_{i=3}^{m-1} t_i = q+(m-2)(j-1)$, $j \leq t_2+1 \leq q-1$ as $t_2 < q-1$, $j \leq t_i \leq q-1$ for $3 \leq i \leq m-1$, and $j \leq t_1+t_m-j \leq q-1$. By the induction hypothesis, $S_{m-1} = \Gamma_{m-1}^+$, and so

$$\mathbf{w} \in \Gamma_{m-1}^+.$$

By Proposition 3, $\mathbf{w}$ is minimal in $\{\mathbf{p} \in H_{m-1} : p_1 = (t_1+t_m-j-j)(q+1)+j\}$. This leads to a contradiction as

$$\begin{aligned}&\mathbf{v} \in \{\mathbf{p} \in H_{m-1} : p_1 = (t_1+t_m-j-j)(q+1)+j\},\\&\mathbf{v} \preceq \mathbf{w}, \text{ and}\\&\mathbf{v} \neq \mathbf{w}.\end{aligned}$$

Since both cases (1) and (2) yield a contradiction, it must be the case that $\boldsymbol{\gamma}_{\mathbf{t},j}$ is minimal in $\{\mathbf{p} \in H_m : p_1 = (t_1-j)(q+1)+j\}$. Therefore, by the definition of Γ_m^+, we have that $\boldsymbol{\gamma}_{\mathbf{t},j} \in \Gamma_m^+$. This completes the proof of the claim that

$$S_m \subseteq \Gamma_m^+.$$

Next, we will show that $\Gamma_m^+ \subseteq S_m$. Suppose not; that is, suppose that there exists $\mathbf{n} \in \Gamma_m^+ \setminus S_m$. Then there exists $f \in \mathbb{F}_{q^2}(X)$ with pole divisor $(f)_\infty = n_1P_1 + \cdots + n_mP_m$. By Lemma 4,

$$\mathbf{n} \in \Gamma_m^+ \subseteq G(P_1) \times G(P_2) \times \cdots \times G(P_m).$$

Thus,

$$\mathbf{n} = ((t_1 - j_1)(q+1) + j_1, (t_2 - j_2)(q+1) + j_2, \ldots, (t_m - j_m)(q+1) + j_m)$$

where $1 \leq j_i \leq t_i \leq q-1$ for all $1 \leq i \leq m$. Without loss of generality, we may assume that $j_m = \max\{j_i : 2 \leq i \leq m\}$ as a similar argument holds if $j_r = \max\{j_i : 2 \leq i \leq m\}$ for some $2 \leq r \leq m-1$. Then

$$(f h_m^{t_m - j_m + 1})_\infty = (n_1 + (t_m - j_m + 1)(q+1))P_1 + \sum_{i=2}^{m-1} n_i P_i,$$

which implies that $(n_1 + (t_m - j_m + 1)(q+1), n_2, \ldots, n_{m-1}) \in H_{m-1}$. Then there exists $\mathbf{u} \in \Gamma_{m-1}$ such that

$$\mathbf{u} \preceq (n_1 + (t_m - j_m + 1)(q+1), n_2, \ldots, n_{m-1})$$

and $u_2 = n_2 = (t_2 - j_2)(q+1) + j_2$. If $u_1 \leq n_1$, then $(u_1, \ldots, u_{m-1}, 0) \preceq \mathbf{n}$ which contradicts the minimality of $\mathbf{n}$ in $\{\mathbf{p} \in H_m : p_2 = n_2\}$. Thus, $u_1 > n_1 > 0$. By the induction hypothesis,

$$\mathbf{u}^+ = \boldsymbol{\gamma}_{(T_{i_1}, \ldots, T_{i_l}), j'} \in S_l = \Gamma_l^+$$

for some l, $2 \leq l \leq m-1$, and some $(T_{i_1}, \ldots, T_{i_l})$ and j' satisfying $1 \leq j' \leq T_{i_r} \leq q-1$ for $1 \leq r \leq l$ and $\sum_{r=1}^{l} T_{i_r} = q + (l-1)(j'-1)$. Hence, there exists an index set $\{i_1, \ldots, i_{m-1}\} = \{1, \ldots, m-1\}$ such that $i_1 < i_2 < \cdots < i_l$ and

$$u_{i_r} = \begin{cases} (T_{i_r} - j')(q+1) + j' & \text{if } 1 \leq r \leq l \\ 0 & \text{if } l+1 \leq r \leq m-1 \end{cases}.$$

Since $u_1 > n_1 > 0$, $i_1 = 1$. Similarly, $i_2 = 2$ because $u_2 = n_2 \neq 0$. Since

$$(T_2 - j')(q+1) + j' = u_{i_2} = u_2 = (t_2 - j_2)(q+1) + j_2$$

implies that $(q+1) \mid (j' - j_2)$, we must have that $j' = j_2$ as $-(q-1) \leq j' - j_2 \leq q-1$. In addition, $T_2 = t_2$. As a result,

$$\mathbf{u}^+ = \boldsymbol{\gamma}_{(T_1, T_2, T_{i_3}, \ldots, T_{i_l}), j_2},$$

$$u_{i_r} = \begin{cases} (T_{i_r} - j_2)(q+1) + j_2 & \text{if } 1 \leq r \leq l \\ 0 & \text{if } l+1 \leq r \leq m-1 \end{cases},$$

$T_1 + T_2 + T_{i_3} + \cdots + T_{i_l} = q + (l-1)(j_2 - 1)$, and $j_2 \leq T_{i_r} \leq q-1$ for all $1 \leq r \leq l$. At this point, we separate the remainder of the proof into two cases:

$$\begin{array}{l} (1)\ u_1 - (t_m - j_m + 1)(q+1) \geq 0 \\ (2)\ u_1 - (t_m - j_m + 1)(q+1) < 0 \end{array}$$

Case (1): Suppose $u_1 - (t_m - j_m + 1)(q+1) \geq 0$. Since $q+1 \nmid j_2$, it follows that $u_1 - (t_m - j_m + 1)(q+1) > 0$. Set

$$\mathbf{v} := (u_1 - (t_m - j_m + 1)(q+1), u_2, u_3, \ldots, u_{m-1}, (t_m - j_m + j_2 - j_2)(q+1) + j_2).$$

Notice that $\mathbf{v} \preceq \mathbf{n}$ since $u_1 \leq n_1 + (t_m - j_m + 1)(q+1)$, $u_i \leq n_i$ for $2 \leq i \leq m-1$, and $j_2 \leq j_m = \max\{j_i : 2 \leq i \leq m\}$. We claim that $\mathbf{v}^+ \in S_{l+1}$. To see this, it is helpful to express $\mathbf{v}^+$ as

$$\mathbf{v}^+ = \gamma_{(T_1 - t_m + j_m - 1, T_2, T_{i_3}, \ldots, T_{i_l}, t_m - j_m + j_2), j_2}.$$

It is easy to see that $T_1 - t_m + j_m - 1 + T_2 + T_{i_3} + \cdots + T_{i_l} + t_m - j_m + j_2 = q + l(j_2 - 1)$, $T_1 - (t_m - j_m) - 1 \leq T_1 \leq q-1$, $j_2 \leq T_{i_r} \leq q-1$ for $2 \leq r \leq l$, and $j_2 \leq t_m - j_m + j_2 \leq t_m \leq q-1$ as $j_2 \leq j_m$. If $T_1 - t_m + j_m - 1 < j_2$, then $u_1 - (t_m - j_m + 1)(q+1) = (T_1 - j_2 - (t_m - j_m + 1))(q+1) + j_2 < 0$ which is not the case. Thus, $j_2 \leq T_1 - t_m + j_m - 1$, establishing the claim that $\mathbf{v}^+ \in S_{l+1}$. Since $S_{l+1} \subseteq \Gamma_{l+1}^+ \subseteq H_{l+1}$, it follows that $\mathbf{v} \in \Gamma_m \subseteq H_m$. Now, $\mathbf{v} \preceq \mathbf{n}$ and $\mathbf{n} \in \Gamma_m^+$ force $\mathbf{n} = \mathbf{v}$ as otherwise $\mathbf{n}$ is not minimal in $\{\mathbf{p} \in H_m : p_2 = n_2\}$. Hence, $l + 1 = m$ and $\mathbf{n} = \mathbf{v} = \mathbf{v}^+ \in S_m$, which is a contradiction.

Case (2): Suppose that $u_1 - (t_m - j_m + 1)(q+1) < 0$. There are two subcases to consider:

(a) $j_1 < t_1$.
(b) $j_1 = t_1$.

Subcase (a): Suppose $j_1 < t_1$. Set

$$\mathbf{v} := ((t_1 - j_1 + j_2 - 1 - j_2)(q+1) + j_2, u_2, \ldots, u_{m-1}, (T_1 - t_1 + j_1 - j_2)(q+1) + j_2).$$

Notice that $\mathbf{v} \preceq \mathbf{n}$ and $\mathbf{v} \neq \mathbf{n}$ since $(t_1 - j_1 - 1)(q+1) + j_2 \leq (t_1 - j_1)(q+1) \leq (t_1 - j_1)(q+1) + j_1$, $u_i \leq n_i$ for $2 \leq i \leq m-1$, and $u_1 < (t_m - j_m + 1)(q+1)$ implies that $T_1 - j_2 \leq t_m - j_m$ which leads to $(T_1 - t_1 + j_1 - j_2)(q+1) + j_2 \leq (t_m - j_m)(q+1) + j_m$ as $j_2 \leq j_m$. The fact that $j_1 < t_1$ gives $\mathbf{v}^+ \in \mathbb{N}^{l+1}$. We claim that $\mathbf{v}^+ \in S_{l+1}$. To see this, it is helpful to express $\mathbf{v}^+$ as

$$\mathbf{v}^+ = \gamma_{(t_1 - j_1 + j_2 - 1, T_2, T_{i_3}, \ldots, T_{i_l}, T_1 - t_1 + j_1), j_2}.$$

It is easy to see that $t_1 - j_1 + j_2 - 1 + T_2 + T_{i_3} + \cdots + T_{i_l} + T_1 - t_1 + j_1 = q + l(j_2 - 1)$, $j_2 \leq T_{i_r} \leq q-1$ for $2 \leq r \leq l$, $j_2 \leq t_1 - j_1 + j_2 - 1$ as $j_1 < t_1$, and $T_1 - (t_1 - j_1) \leq q - 1$. In order to conclude that $\mathbf{v}^+ \in S_{l+1}$, it only remains to show that $t_1 - j_1 + j_2 - 1 \leq q - 1$ and $j_2 \leq T_1 - t_1 + j_1$. It suffices to show that $j_2 \leq T_1 - t_1 + j_1$ since this implies that $j_2 \leq q - (t_1 - j_1)$ and so $t_1 - j_1 + j_2 - 1 \leq q - 1$. If $j_2 > T_1 - t_1 + j_1$, then $(T_1 - j_2)(q+1) < (t_1 - j_1)(q+1) + j_1 - j_2$, contradicting the fact that $u_1 > n_1$. Hence, $j_2 \leq T_1 - t_1 + j_1$ and $\mathbf{v}^+ \in S_{l+1} \subseteq \Gamma_{l+1}^+ \subseteq H_{l+1}$. It follows that $\mathbf{v} \in H_m$ and so $\mathbf{v} \in \{\mathbf{p} \in H_m : p_2 = n_2\}$. This yields a contradiction as $\mathbf{n}$ is minimal in $\{\mathbf{p} \in H_m : p_2 = n_2\}$, concluding the proof in this subcase.

Subcase (b): Suppose that $j_1 = t_1$. Set

$$\mathbf{v} := (0, u_2, \ldots, u_{m-1}, (T_1 - j_2)(q+1) + j_2).$$

Then $\mathbf{v} \preceq \mathbf{n}$ and $\mathbf{v} \neq \mathbf{n}$ since $0 < n_1$, $u_i \leq n_i$ for $2 \leq i \leq m-1$, and $u_1 < (t_m - j_m + 1)(q+1)$ implies $T_1 - j_2 \leq t_m - j_m$ which means $(T_1 - j_2)(q+1) + j_2 \leq (t_m - j_m)(q+1) + j_m$ as $j_2 \leq j_m$. It is easy to see that $\mathbf{v}^+ \in S_l$ as $\sum_{r=1}^{l} T_{i_r} = q + (l-1)(j_2 - 1)$ and $j_2 \leq T_{i_r} \leq q-1$ for all $1 \leq r \leq l$. As before, it follows that $\mathbf{v} \in H_m$ and $\mathbf{v} \in \{\mathbf{p} \in H_m : p_2 = n_2\}$. Since $\mathbf{v} \neq \mathbf{n}$, this contradicts the minimality of $\mathbf{n}$ in the set $\{\mathbf{p} \in H_m : p_2 = n_2\}$, concluding the proof in this subcase.

Since both cases (1) and (2) yield a contradiction, it must be the case that no such $\mathbf{n}$ exists. Hence, $\Gamma_m^+ \setminus S_m = \emptyset$. This establishes that $\Gamma_m^+ \subseteq S_m$, concluding the proof that $\Gamma_m^+ = S_m$.

To illustrate Theorem 10, we provide an example.

Example 11. As in Example 5, consider the curve X defined by $y^8 + y = x^9$ over $\mathbb{F}_{64} = \mathbb{F}_2(\omega)$ where $\omega^6 + \omega^4 + \omega^3 + \omega + 1 = 0$. Let $P_1 = P_\infty$, $P_2 = P_{00}$, $P_3 = P_{01}$, $P_4 = P_{0\omega^9}$. Since $\Gamma_1 = \langle 8, 9 \rangle$ and Γ_2^+ is described in Example 5, to determine $H(P_1, P_2, P_3)$ it only remains to find Γ_3^+. By Theorem 10, $\Gamma_3^+ =$

$$\left\{ \begin{array}{l} (1,1,46),(1,10,37),(1,19,28),(1,28,19),(1,37,10),(1,46,1), \\ (2,2,38),(2,11,29),(2,20,20),(2,29,11),(2,38,2), \\ (3,3,30),(3,12,21),(3,21,12),(3,30,3), \\ (4,4,22),(4,13,13),(4,22,4), \\ (5,5,14),(5,14,5),(6,6,6), \\ (10,1,37),(10,10,28),(10,19,19),(10,28,10),(10,37,1), \\ (11,2,29),(11,11,20),(11,20,11),(11,29,2), \\ (12,3,21),(12,12,12),(12,21,3), \\ (13,4,13),(13,13,4), \\ (14,5,5), \\ (19,1,28),(19,10,19),(19,19,10),(19,28,1), \\ (20,2,20),(20,11,11),(20,20,2), \\ (21,3,12),(21,12,3), \\ (22,4,4), \\ (28,1,19),(28,10,10),(28,19,1), \\ (29,2,11),(29,11,2), \\ (30,3,3), \\ (37,1,10),(37,10,1), \\ (38,2,2), \\ (46,1,1) \end{array} \right\}.$$

To find $H(P_1, P_2, P_3, P_4)$, we only need to apply Theorem 10 to see that $\Gamma_4^+ =$

$$\left\{ \begin{array}{l} (1,1,1,37),(1,1,10,28),(1,1,19,19),(1,1,28,10),(1,1,37,1),(1,10,1,28), \\ (1,10,10,19),(1,10,19,10),(1,10,28,1),(1,19,1,19),(1,19,10,10),(1,19,19,1), \\ (1,28,1,10),(1,28,10,1),(1,37,1,1), \\ (2,2,2,29),(2,2,11,20),(2,2,20,11),(2,2,29,2),(2,11,2,20),(2,11,11,11), \\ (2,11,20,2),(2,20,2,11),(2,20,11,2),(2,29,2,2), \\ (3,3,3,21),(3,3,12,12),(3,3,21,3),(3,12,3,12),(3,12,12,3),(3,21,3,3), \\ (4,4,4,13),(4,4,13,4),(4,13,4,4), \\ (5,5,5,5), \\ (10,1,1,28),(10,1,10,19),(10,1,19,10),(10,1,28,1),(10,10,1,19),(10,10,10,10), \\ (10,10,19,1),(10,19,1,10),(10,19,10,1),(10,28,1,1), \\ (11,2,2,20),(11,2,11,11),(11,2,20,2),(11,11,2,11),(11,11,11,2),(11,20,2,2), \\ (12,3,3,12),(12,3,12,3),(12,12,3,3), \\ (13,4,4,4), \\ (19,1,1,19),(19,1,10,10),(19,1,19,1),(19,10,1,10),(19,10,10,1),(19,19,1,1), \\ (20,2,2,11),(20,2,11,2),(20,11,2,2), \\ (21,3,3,3), \\ (28,1,1,10),(28,1,10,1),(28,10,1,1), \\ (29,2,2,2), \\ (37,1,1,1) \end{array} \right\}.$$

Similarly, one can use Theorem 10 to find Γ_5^+, Γ_6^+, Γ_7^+, Γ_8^+, and Γ_9^+.

4 Acknowledgements

The author wishes to thank the anonymous referee whose careful reading and detailed comments led to numerous improvements in the proof of Theorem 10. This project was supported by NSF grant DMS-0201286 and an ORAU Ralph E. Powe Junior Faculty Enhancement Award.

References

1. E. Arbarello, M. Cornalba, P. Griffiths, and J. Harris, *Geometry of Algebraic Curves*, Springer-Verlag, 1985.
2. E. Ballico and S. J. Kim, *Weierstrass multiple loci of n-pointed algebraic curves*, J. Algebra **199** (1998), 455–471.
3. C. Carvalho and F. Torres, *On Goppa codes and Weierstrass gaps at several points*, preprint.
4. A. Garcia, S. J. Kim, and R. F. Lax, *Consecutive Weierstrass gaps and minimum distance of Goppa codes*, J. Pure Appl. Algebra **84** (1993), 199–207.
5. M. Homma, *The Weierstrass semigroup of a pair of points on a curve*, Arch. Math. **67** (1996), 337–348.
6. M. Homma and S. J. Kim, *Goppa codes with Weierstrass pairs*, J. Pure Appl. Algebra **162** (2001), 273–290.
7. S. J. Kim, *On the index of the Weierstrass semigroup of a pair of points on a curve*, Arch. Math. **62** (1994), 73–82.

8. H. Maharaj, G. L. Matthews, and G. Pirsic, *Riemann-Roch spaces for the Hermitian function field with applications to low-discrepency sequences and algebraic geometry codes*, preprint.
9. G. L. Matthews, *Weierstrass pairs and minimum distance of Goppa codes*, Des. Codes and Cryptog. **22** (2001), 107–121.
10. G. L. Matthews, *Weierstrass pairs and minimum distance of Goppa codes*, Ph.D. dissertation, Louisiana State University, Baton Rouge, Louisiana, USA, May 1999.