WEIERSTRASS SEMIGROUPS AND CODES FROM A QUOTIENT OF THE HERMITIAN CURVE

GRETCHEN L. MATTHEWS
DEPARTMENT OF MATHEMATICAL SCIENCES
CLEMSON UNIVERSITY
CLEMSON, SC 29634-0975
U.S.A.
E-MAIL: GMATTHE@CLEMSON.EDU

Abstract. We consider the quotient of the Hermitian curve defined by the equation $y^q + y = x^m$ over $\mathbb{F}_{q^2}$ where $m > 2$ is a divisor of $q+1$. For $2 \leq r \leq q+1$, we determine the Weierstrass semigroup of any r-tuple of $\mathbb{F}_{q^2}$-rational points $(P_\infty, P_{0b_2}, \ldots, P_{0b_r})$ on this curve. Using these semigroups, we construct algebraic geometry codes with minimum distance exceeding the designed distance. In addition, we prove that there are r-point codes, that is codes of the form $C_\Omega(D, \alpha_1 P_\infty + \alpha_2 P_{0b_2} + \cdots + \alpha_r P_{0b_r})$ where $r \geq 2$, with better parameters than any comparable one-point code on the same curve. Some of these codes have better parameters than comparable one-point Hermitian codes over the same field. All of our results apply to the Hermitian curve itself which is obtained taking $m = q+1$ in the above equation.

1. Introduction

Algebraic geometry codes, as defined by Goppa in [6], [7], are linear codes formed using two divisors G and D on a curve. Typically, the divisor G is taken to be a multiple of a single point P and the code is called a one-point code. The parameters of such codes are closely related to the Weierstrass semigroup of the point P [4]. It has been shown that one may obtain codes with better parameters by allowing the divisor G to be more general (see [14], [9], [3], [18]). In particular, if G is a divisor supported by r points, then one can use the Weierstrass semigroup of the r-tuple of these points to estimate the parameters of the associated r-point code. While the Weierstrass semigroup of an r-tuple of points is a generalization of the classically studied Weierstrass semigroup of a point, very little is known about this set if $r \geq 2$ (see [11], [8], [2]). The only families of curves over a finite field for which the Weierstrass semigroup of even a pair of points has been determined are the families of hyperelliptic and plane quartic curves [11], Hermitian [14], and Suzuki curves [13]. In this work, we provide techniques for determining Weierstrass semigroups of r-tuples of distinct points on an arbitrary curve by expounding on the work of Carvalho and Torres [3]. To illustrate these techniques, we determine the Weierstrass semigroup of certain r-tuples of points on a quotient of the Hermitian curve for $2 \leq r \leq q+1$. This is a generalization of the main result of [15] where

Key words and phrases. Weierstrass semigroup, Weierstrass gap, algebraic geometry code, Hermitian curve.

This project was supported by NSF grant DMS-0201286.

the Weierstrass semigroup of an r-tuple of collinear points on a Hermitian curve is described.

In this paper, we consider the curve X over $\mathbb{F}_{q^2}$ defined by $y^q + y = x^m$ where $m > 2$ is a divisor of $q+1$. This curve was originally studied by F. K. Schmidt [16] as the first known example of a non-classical curve. In [5], it is shown that X is a maximal curve meaning that the number of $\mathbb{F}_{q^2}$-rational points on X is equal to the Weil upper bound. Hence, it is natural to use this curve to construct algebraic geometry codes. Another motivation for the study of this curve and associated codes is that if one takes $m = q+1$, the much-studied Hermitian curve is obtained.

This paper is organized as follows. Section 2 contains basic facts about the curve we will study as well as notation to be used throughout this paper. In Section 3, we describe the minimal generating set of a Weierstrass semigroup of an r-tuple of points on an arbitrary curve. As an application, we determine the Weierstrass semigroup of any r-tuple of points of the form $(P_\infty, P_{0b_2}, \ldots, P_{0b_r})$ on the quotient of the Hermitian curve defined by $y^q + y = x^m$ over $\mathbb{F}_{q^2}$, where $2 \leq r \leq q+1$. This semigroup is utilized in Section 4 where we construct algebraic geometry codes supported by the r points $P_\infty, P_{0b_2}, \ldots, P_{0b_r}$ and compare them with one-point codes from the same curve. This section also contains results on using the semigroup of an r-tuple of points to better estimate the minimum distance of codes supported by r points and comparisons of codes constructed using a quotient of the Hermitian curve with Hermitian codes over the same field.

2. Notation and Preliminaries

In this section, we introduce notation to be used throughout this work. Then some facts from [5] concerning a quotient of the Hermitian curve are reviewed.

Let X be a projective curve of genus g 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 (resp. differential η) will be denoted by (f) (resp. (η)). The divisor of poles of f will be denoted by $(f)_\infty$. Given a divisor A on X defined over $\mathbb{F}$, let $\mathcal{L}(A)$ denote the set of rational functions f on X defined over $\mathbb{F}$ with divisor $(f) \geq -A$ together with the zero function and $\Omega(A)$ denote the set of rational differentials η on X defined over $\mathbb{F}$ with divisor $(\eta) \geq A$ together with the zero differential. Let $\ell(A)$ denote the dimension of $\mathcal{L}(A)$ as an $\mathbb{F}$-vector space. Two divisors D_1 and D_2 are said to be linearly equivalent, denoted $D_1 \sim D_2$, if $D_1 - D_2 = (f)$ for some rational function f.

Algebraic geometry codes $C_{\mathcal{L}}(D, G)$ and $C_\Omega(D, G)$ can be constructed using divisors $D = \sum_{i=1}^n Q_i$ and $G = \sum_{i=1}^r \alpha_i P_i$ on X where $Q_1, \ldots, Q_n, P_1, \ldots, P_r$ are pairwise distinct $\mathbb{F}$-rational points and $\alpha_i \in \mathbb{N}$ for all i, $1 \leq i \leq r$. In particular,

$$C_{\mathcal{L}}(D, G) := \{(f(Q_1), \ldots, f(Q_n)) : f \in \mathcal{L}(G)\}$$

and

$$C_\Omega(D, G) := \{(res_{Q_1}(\eta), \ldots, res_{Q_n}(\eta)) : \eta \in \Omega(G - D)\}.$$

We will refer to these codes as r-point codes since the divisor G has r distinct $\mathbb{F}$-rational points in its support. Typically, an r-point code is constructed by taking the divisor D to be the sum of all $\mathbb{F}$-rational points not in the support of G, and we will keep this convention. If $\deg G < n$, then $C_{\mathcal{L}}(D, G)$ has length n, dimension $\ell(G)$, and designed distance $n - \deg G$. If $\deg G > 2g - 2$, then $C_\Omega(D, G)$ has dimension $\ell(K + D - G)$, where K is a canonical divisor, and designed distance

$\deg G - (2g-2)$. The minimum distance of each of the codes $C_{\mathcal{L}}(D,G)$ and $C_{\Omega}(D,G)$ is at least its designed distance. A code of length n, dimension k, and minimum distance d (resp. at least d) is called an $[n,k,d]$ (resp. $[n,k,\geq d]$) code.

We now focus our attention on the curve X defined by $y^q + y = x^m$ over $\mathbb{F}_{q^2}$ where q is a prime power, m is a divisor of $q+1$, and $m > 2$. In all that follows, we let c denote the quotient $c := \frac{q+1}{m}$ and we set $l := \min\{m, q\}$. It can be shown that the genus of X is $g := \frac{(m-1)(q-1)}{2}$. Since $\mathbb{F}_{q^2}^* := \mathbb{F}_{q^2} \setminus \{0\}$ is cyclic, there is a unique subgroup H of $\mathbb{F}_{q^2}^*$ of order $m(q-1)$. The $\mathbb{F}_{q^2}$-rational points on X are $P_{ab} := (a : b : 1)$, where $a, b \in \mathbb{F}_{q^2}$ satisfy $b^q + b = a^m$, and a single point at infinity, denoted P_∞. In fact, for each $a \in H \cup \{0\}$, there are exactly q $\mathbb{F}_{q^2}$-rational points P_{ab} on X. This together with the Weil bound shows that X has exactly $q(m(q-1)+1)+1$ $\mathbb{F}_{q^2}$-rational points. One may notice that $P_\infty = (0:1:0)$ if $m = q+1$, and $P_\infty = (1:0:0)$ if $m \neq q+1$.

3. The minimal generating set of a Weierstrass semigroup

In this section, we consider Weierstrass semigroups of r-tuples of points. We begin by discussing the notion of the minimal generating set of a Weierstrass semigroup of an r-tuple of points on an arbitrary curve X. Then we restrict our attention to the quotient of the Hermitian curve described in Section 2 and determine the minimal generating set for any r-tuple of $\mathbb{F}_{q^2}$-rational points of the form $(P_\infty, P_{0b_2}, \ldots, P_{0b_r})$ where $2 \leq r \leq q+1$.

Let X be a curve over $\mathbb{F}$ of genus $g > 1$. Given r distinct $\mathbb{F}$-rational points $P_1, \ldots, P_r$ on the curve X, the Weierstrass semigroup $H(P_1, \ldots, P_r)$ of the r-tuple $(P_1, \ldots, P_r)$ is defined by

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

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

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

where $\mathbb{N}_0 := \mathbb{N} \cup \{0\}$ denotes the set of nonnegative integers. When the context is clear, we may write $H_r := H(P_1, \ldots, P_r)$ and $G_r := G(P_1, \ldots, P_r)$ even though both of these sets depend on the points $P_1, \ldots, P_r$. If $m = 1$, the Weierstrass gap set is the classically studied gap sequence and $\mid G(P_1) \mid = g$, the genus of X. In general, if $r \geq 2$, then $\mid G(P_1, \ldots, P_r) \mid$ depends on the choice of points $P_1, \ldots, P_r$ [1]. However, as we shall see, any r-tuple of distinct points of the form $(P_\infty, P_{0b_2}, \ldots, P_{0b_r})$ on the quotient of the Hermitian curve with defining equation $y^q + y = x^m$ has the same Weierstrass gap set. Moreover, a minimal generating set for the Weierstrass semigroup $H(P_\infty, P_{0b_2}, \ldots, P_{0b_r})$ is given. Before we do this, let us review some results on computing Weierstrass semigroups and set up some notation strongly inspired by [3].

Define a partial order $\preceq$ on $\mathbb{N}_0^r$ 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 $\mathbb{N}_0^r$, we will always do so with respect to the partial order $\preceq$. Given $\mathbf{v} := (v_1, \ldots, v_r) \in \mathbb{Z}^r$, let

$$\tilde{\mathbf{v}} := (v_{i_1}, \ldots, v_{i_l}) \in \mathbb{N}^l$$

where $i_1 < \cdots < i_l$ and $v_i > 0$ if and only if $i = i_j$ for some $1 \leq j \leq l$; that is, $\tilde{\mathbf{v}}$ is the vector formed from $\mathbf{v}$ by deleting each coordinate of $\mathbf{v}$ containing a negative or

zero entry. Given $\mathbf{u_1}, \ldots, \mathbf{u_l} \in \mathbb{N}_0^r$, define the least upper bound of $\mathbf{u_1}, \ldots, \mathbf{u_l}$ by

$$\text{lub}\{\mathbf{u_1}, \ldots, \mathbf{u_l}\} = (\max\{u_{1_1}, \ldots, u_{l_1}\}, \ldots, \max\{u_{1_r}, \ldots, u_{l_r}\}) \in \mathbb{N}_0^r.$$

We will see that Weierstrass semigroups are generated by taking least upper bounds of elements in certain sets. These sets can be defined in the following manner. Let $\tilde{\Gamma}(P_1) := H(P_1)$. For $2 \leq r \leq q+1$, define

$$\tilde{\Gamma}(P_1, \ldots, P_r) := \left\{ \mathbf{n} \in \mathbb{N}^r : \begin{array}{c} \mathbf{n} \text{ is minimal in } \{\mathbf{p} \in H_r : p_i = n_i\} \\ \text{for some } i, 1 \leq i \leq r \end{array} \right\}.$$

For $1 \leq r \leq q+1$, set

$$\Gamma(P_1, \ldots, P_r) := \left\{ \mathbf{n} \in \mathbb{N}_0^r : \begin{array}{c} \tilde{\mathbf{n}} = (n_{i_1}, \ldots, n_{i_k}) \in \tilde{\Gamma}(P_{i_1}, \ldots, P_{i_k}) \\ \text{for some } 1 \leq k \leq r \text{ and } 1 \leq i_1 < \cdots < i_k \leq r \end{array} \right\}.$$

If the context is clear, we may write $\tilde{\Gamma}_r := \tilde{\Gamma}(P_1, \ldots, P_r)$ and $\Gamma_r := \Gamma(P_1, \ldots, P_r)$.

Lemma 3.1. [15, Proposition 3] *Let $P_1, \ldots, P_r$ be distinct $\mathbb{F}$-rational points on a curve X. Then*

$$\tilde{\Gamma}_r = \{\mathbf{n} \in \mathbb{N}^r : \mathbf{n} \text{ is minimal in } \{\mathbf{p} \in H_r : p_i = n_i\} \text{ for all } i, 1 \leq i \leq r\}.$$

The following result describes how the set Γ_r generates the entire Weierstrass semigroup $H(P_1, \ldots, H_r)$.

Theorem 3.2. [15, Theorem 7] *Let $P_1, \ldots, P_r$ be distinct $\mathbb{F}$-rational points on a curve X. If $1 \leq r \leq |\mathbb{F}|$, then*

$$H(P_1, \ldots, P_r) = \{\text{lub}\{\mathbf{u_1}, \ldots, \mathbf{u_r}\} \in \mathbb{N}_0^r : \mathbf{u_1}, \ldots, \mathbf{u_r} \in \Gamma_r\}.$$

We will refer to Γ_r as the minimal generating set of the Weierstrass semigroup $H(P_1, \ldots, P_r)$. According to Theorem 3.2, to determine $H(P_1, \ldots, P_r)$, we only need to determine $\tilde{\Gamma}(P_{i_1}, \ldots, P_{i_k})$ for all $1 \leq i_1 < \cdots < i_k \leq r$ and $1 \leq k \leq r$. This is precisely what we will do for certain r-tuples of $\mathbb{F}_{q^2}$-rational points on the curve X defined by $y^q + y = x^m$ where m is a divisor of $q+1$ and $m > 2$.

Let $P_1 = P_\infty, P_2 = P_{0b_2}, P_3 = P_{0b_3}, \ldots, P_{q+1} = P_{0b_{q+1}}$ be $q+1$ distinct $\mathbb{F}_{q^2}$-rational points on the curve X. Let $a \in H \cup \{0\}$ and $b \in \mathbb{F}_{q^2}$. To compute the Weierstrass semigroups, we will make use of the following principal divisors of X [5]:

$$\begin{aligned} (x-a) &= \sum_{\substack{b \in \mathbb{F}_{q^2} \\ b^q + b = a^m}} P_{ab} - qP_\infty \\ (y-b) &= \begin{cases} mP_{0b} - mP_\infty & \text{if } b^q + b = 0 \\ \sum_{\substack{a \in \mathbb{F}_{q^2} \\ b^q + b = a^m}} P_{ab} - mP_\infty & \text{if } b^q + b = a^m \text{ where } a \in H. \end{cases} \end{aligned}$$

Using these functions together with the fact that $|G(P)| = \frac{(m-1)(q-1)}{2}$, one can obtain the following result.

Proposition 3.3. [5, Theorem 3] *The Weierstrass semigroup of any $\mathbb{F}_{q^2}$-rational point P_{0b} or P_∞ on the curve defined by $y^q + y = x^m$ where $m > 2$ is a divisor of $q+1$ is $H(P_{0b}) = H(P_\infty) = \langle m, q \rangle$.*

According to the above proposition, the $\mathbb{F}_{q^2}$-rational points P_∞ and P_{0b} on X have the same gap set $\mathbb{N} \setminus \langle m, q \rangle$. Since $\langle m, q \rangle$ is a symmetric semigroup with largest

gap $mq-m-q$, a positive integer $\alpha \leq mq-m-q$ is not an element of $\langle m,q\rangle$ if and only if $mq-m-q-\alpha \in \langle m,q\rangle$. Using this fact, we see that

$$G(P_{0b}) = G(P_\infty) = \left\{ (t-j)m+j : \begin{array}{l} 1 \leq j \leq l-1, \\ j \leq t \leq q-1-j(c-1) \end{array} \right\}$$

where $l = \min\{m,q\}$. We will now describe a convenient way to organize the elements of this gap set. Recall that $c = \frac{q+1}{m}$. Write the integers $1,2,\ldots,l-1$ in a row. For each $1 \leq j \leq l-1$, form a column, Column j, with first entry j by adding multiples of m to j: j, $j+m$, $j+2m$, $\ldots$,$j+(q-1-jc)m$. This gives

1	2	$\cdots$	j	$\cdots$	$l-1$
$m+1$	$m+2$	$\cdots$	$m+j$	$\cdots$	$m+(l-1)$
					$\vdots$
					$(q-1-(l-1)c)m+l-1$
				$\iddots$	
		$\iddots$	$(q-1-jc)m+j$		
	$(q-1-2c)m+2$				
$(q-1-c)m+1$					

Assign labels $1,\ldots,q-1-c$ to the diagonals running from the bottom left to upper right (i.e., those running in the direction of $\nearrow$) starting at the upper left corner. In doing this, we allow blank entries along these diagonals. Notice that if $\alpha = (t-j)m+j$ with $1 \leq j \leq l-1$ and $1 \leq j \leq t \leq q-1-j(c-1)$, then α is on the t^{th} diagonal and in the j^{th} column of the above diagram. Also note that if $m = q+1$ then this diagram is the familiar "triangle of gaps" of any $\mathbb{F}_{q^2}$-rational point of the Hermitian curve over $\mathbb{F}_{q^2}$. It is worth pointing out that if $m \neq q+1$ then not all $\mathbb{F}_{q^2}$-rational points on X have the same gap set. Hence, it is necessary to restrict ourselves to the $\mathbb{F}_{q^2}$-rational points P_∞ and P_{0b} where $b^q+b=0$.

The next result describes the minimal generating set for the Weierstrass semigroup of the pair (P_∞, P_{0b}) of $\mathbb{F}_{q^2}$-rational points on X. Although the case $b=0$ is the content of [11, Lemma 5.2], we include a proof here for any $b \in \mathbb{F}_{q^2}$ such that $b^q+b=0$. As a special case of this result, we obtain [14, Theorem 3.4] where the Weierstrass semigroup of a pair of $\mathbb{F}_{q^2}$-rational points on the Hermitian curve is determined.

Proposition 3.4. *Let $P_1 = P_\infty$ and $P_2 = P_{0b}$ be $\mathbb{F}_{q^2}$-rational points on the curve $y^q+y=x^m$ where $m>2$ is a divisor of $q+1$. Then*

$$\tilde{\Gamma}_2 = \left\{ ((t_1-j)m+j, (t_2-j)m+j) : \begin{array}{l} 1 \leq j \leq l-1, \\ j \leq t_1, t_2 \leq q-1-j(c-1), \\ t_1+t_2 = (m-j)c+2(j-1) \end{array} \right\}.$$

Therefore, $H(P_1,P_2)$ is generated by

$$\tilde{\Gamma}_2 \times \cup \left(\langle m,q\rangle \times \{0\} \right) \cup \left(\{0\} \times \langle m,q\rangle \right).$$

Proof. If $1 \leq j \leq l-1$, $j \leq t_1, t_2 \leq q-1-j(c-1)$, and $t_1+t_2 = (m-j)c+2(j-1)$, then

$$\left(\frac{x^{m-j}}{(y-b)^{t_2-j+1}} \right)_\infty = ((t_1-j)m+j)P_1 + (t_2-j)m+j)P_2.$$

Therefore,

$$((t_1-j)m+j, (t_2-j)m+j) \in H(P_1,P_2).$$

To see that this gives $\tilde{\Gamma}_2$ as claimed, let

$$\begin{array}{rccc} \phi : & G(P_1) & \to & G(P_2) \\ & \alpha & \mapsto & \beta \end{array}$$

where $(\alpha, \beta) \in \tilde{\Gamma}_2$. Then ϕ defines a one-to-one correspondence [11]. Fix $1 \leq j \leq l-1$ and start with $\alpha = (q-1-jc)m+j$, the last entry in the j^{th} column of the diagram above. We have that $((q-1-jc)m+j, j) \in H(P_1, P_2)$ for $1 \leq j \leq l-1$. Hence, $((q-1-jc)m+j, j) \in \tilde{\Gamma}_2$ for $1 \leq j \leq l-1$. Now consider $\alpha = (q-1-jc-1)m+j$, the next to the last entry in the j^{th} column. Then $((q-1-jc-1)m+j, m+j) \in H(P_1, P_2)$ and so $((q-1-jc-1)m+j, m+j) \in \tilde{\Gamma}_2$ for $1 \leq j \leq l-1$. In general, if α is the k^{th} from the last entry in its particular column, then $\alpha = (q-1-jc-k)m+j$ and we obtain that

$$((q-1-jc-k)m+j, km+j) \in \tilde{\Gamma}_2.$$

Considering this for increasing k, $0 \leq k \leq q-1-jc$, and using the one-to-one correspondence above gives $\tilde{\Gamma}_2$ as claimed. □

Finding the Weierstrass semigroup of the pair (P_∞, P_{0b}) as in Proposition 3.4 lays a foundation for determining the Weierstrass semigroup of r-tuples of the form $(P_\infty, P_{0b_2}, \ldots, P_{0b_r})$. It is interesting to note that each pair in $\tilde{\Gamma}_2$ has coordinates that come from the same column in the diagram of gaps at the points P_1 and P_2. While this is not necessarily the case for an arbitrary curve, we do have the following general result.

Lemma 3.5. [15, Lemma 4] *If $P_1, \ldots, P_r$ are distinct $\mathbb{F}$-rational points on a curve X and $2 \leq r \leq |\, \mathbb{F} \,|$, then $\tilde{\Gamma}(P_1, \ldots, P_r) \subseteq G(P_1) \times \cdots \times G(P_r)$.*

It is convenient to have a compact notation to describe the elements of the minimal generating set of the Weierstrass semigroup $H(P_\infty, P_{0b_2}, \ldots, P_{0b_r})$.

Definition 3.6. *Given $1 \leq r \leq q+1$, $\mathbf{t} = (t_1, \ldots, t_r) \in \mathbb{N}^r$, and $j \in \mathbb{N}$ such that $1 \leq j \leq l-1$ and $j \leq t_i \leq q-1-j(c-1)$ for all $1 \leq i \leq r$, define*

$$\boldsymbol{\gamma}_{\mathbf{t},j} := ((t_1-j)m+j, (t_2-j)m+j, \ldots, (t_r-j)m+j) \in \mathbb{N}^r.$$

We emphasize that the notation $\boldsymbol{\gamma}_{\mathbf{t},j}$ will only be used to describe vectors as defined above where $1 \leq j \leq l-1$ and $j \leq t_i \leq q-1-j(c-1)$ for all $1 \leq i \leq r$. Then

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

We next show that certain $\boldsymbol{\gamma}_{\mathbf{t},j}$ form the minimal generating set of the Weierstrass semigroup $H(P_\infty, P_{0b_2}, \ldots, P_{0b_r})$ for any $2 \leq r \leq q+1$.

Theorem 3.7. *Let $P_1 = P_\infty, P_2 = P_{0b_2}, P_3 = P_{0b_3}, \ldots, P_{q+1} = P_{0b_{q+1}}$ be $q+1$ distinct $\mathbb{F}_{q^2}$-rational points on the curve X defined by $y^q + y = x^m$ where $m > 2$ is a divisor of $q+1$. For $2 \leq r \leq q+1-c$,*

$$\tilde{\Gamma}_r = \left\{ \boldsymbol{\gamma}_{\mathbf{t},j} \in \mathbb{N}^r : \sum_{i=1}^{r} t_i = (m-j)c + r(j-1) \right\},$$

and for $q+1-c < r \leq q+1$,

$$\tilde{\Gamma}_r = \emptyset.$$

In particular, the Weierstrass semigroup $H(P_1, \ldots, P_r)$ is generated by

$$\left\{ \mathbf{n} \in \mathbb{N}_0^r : \tilde{\mathbf{n}} = \boldsymbol{\gamma}_{\mathbf{t},j} \in \tilde{\Gamma}_k \text{ for some } 1 \leq k \leq r \right\}.$$

Hence, the Weierstrass semigroup $H(P_1, \ldots, P_r)$ is

$$H(P_1, \ldots, P_r) = \left\{ \mathrm{lub}\{\mathbf{u_1}, \ldots, \mathbf{u_r}\} : \tilde{\mathbf{u}}_\mathbf{i} \in \tilde{\Gamma}_{k_i}, 1 \leq k_i \leq r \right\}.$$

The proof of Theorem 3.7 is rather technical and so is included in Appendix A. It is interesting to note that each element of $\tilde{\Gamma}_r$ has all entries coming from the same column in the gap diagram. To illustrate this, we include an example.

Example 3.8. Let X denote the curve of genus 7 over $\mathbb{F}_{64}$ defined by $y^8 + y = x^3$ and let

$$(P_1, P_2, \ldots, P_9) := (P_\infty, P_{0b_2}, \ldots, P_{0b_9})$$

be a 9-tuple of distinct $\mathbb{F}_{64}$-rational points on X. Then

$$H(P_1) = \cdots = H(P_9) = \langle 3, 8 \rangle$$

and the Weierstrass gap set of P_i, $1 \leq i \leq 9$, is

$$\begin{array}{cc} 1 & 2 \\ 4 & 5 \\ 7 & \\ 10 & \\ 13. & \end{array}$$

By Proposition 3.4,

$$\tilde{\Gamma}_2 = \left\{ \begin{array}{ll} (1,13), & (2,5), \\ (4,10), & (5,2), \\ (7,7), & \\ (10,4), & \\ (13,1) & \end{array} \right\}$$

To generate the Weierstrass semigroup of the pair (P_1, P_2), one only needs to take least upper bounds of all pairs in the set

$$\Gamma_2 = \tilde{\Gamma}_2 \cup (\{0\} \times \langle 3, 8 \rangle) \cup (\langle 3, 8 \rangle \times \{0\}) .$$

Applying Theorem 3.7, one can obtain that

$$\Gamma_3^+ = \left\{ \begin{array}{l} (1,1,10), (1,4,7), (1,7,4), (1,10,1), (2,2,2), (4,1,7), \\ (4,4,4), (4,7,1), (7,1,4), (7,4,1), (10,1,1) \end{array} \right\},$$

$$\Gamma_4^+ = \left\{ \begin{array}{l} (1,1,1,7), (1,1,4,4), (1,1,7,1), (1,4,1,4), (1,4,4,1), \\ (1,7,1,1), (4,1,1,4), (4,1,4,1), (4,4,1,1), (7,1,1,1) \end{array} \right\},$$

$$\Gamma_5^+ = \{(1,1,1,1,4), (1,1,1,4,1), (1,1,4,1,1), (1,4,1,1,1), (4,1,1,1,1)\} ,$$

and

$$\Gamma_6^+ = \{(1,1,1,1,1,1)\} .$$

Notice also that $\Gamma_7^+ = \Gamma_8^+ = \Gamma_9^+ = \emptyset$. This means that for $7 \leq r \leq 9$,

$$\Gamma_r = \left\{ \mathbf{n} \in \mathbb{N}_0^r : \tilde{\mathbf{n}} \in \cup_{i=1}^6 \Gamma_i^+ \right\} .$$

4. Weierstrass semigroups and r-point codes

In this section, we demonstrate how the semigroup found in Section 3 may be used to construct algebraic geometry codes supported by r points. We will compare these r-point codes with one-point codes from the same curve and with one-point Hermitian codes over the same field. To aid in estimating the parameters of r-point codes, we will use the following generalization of [14, Theorem 2.1]. Note that this result applies to an arbitrary curve. As usual, $\mathbf{e_i} = (0, \ldots, 0, 1, 0, \ldots, 0)$ denotes the unit vector with 1 in the i^{th} coordinate and 0 in all others.

Theorem 4.1. *Let $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{N}_0^r$ and let $G = \sum_{i=1}^r (\alpha_i + \beta_i - 1)P_i$ be a divisor on X supported by r distinct $\mathbb{F}$-rational points. Assume that $\alpha_1 \geq 1$,*

$$\{\mathbf{u} \in \mathbb{N}_0^r : u_1 = \alpha_1, \mathbf{u} \preceq \boldsymbol{\alpha}\} \subseteq G(P_1, \ldots, P_r),$$

and

$$\left\{ \boldsymbol{\beta} - \mathbf{a} - \mathbf{1} + \mathbf{e_1} \in \mathbb{N}_0^r : \mathbf{a} \in \mathbb{N}_0^r, a_1 = 0, \sum_{i=2}^r a_i \leq 2g - 1 - \sum_{i=1}^r \alpha_i \right\} \subseteq G(P_1, \ldots, P_r).$$

Set $D := Q_1 + \cdots + Q_n$, where $Q_1, \ldots, Q_n$ are distinct $\mathbb{F}$-rational points and no Q_i is in the support of G. If the r-point code $C_\Omega(D, G)$ is nontrivial, then the minimum distance of this code is at least $\deg G - (2g-2) + 1$.

We omit the proof of Theorem 4.1 as it is very similar to that of [14, Theorem 2.1]. While the previous result holds for an arbitrary curve, the next result applies only to the quotient of the Hermitian curve X defined by $y^q + y = x^m$ where $m > 2$ is a divisor of $q+1$. Here, if one takes $m = q+1$, then a generalization of [14, Theorem 4.1] is obtained.

Theorem 4.2. *Let $P_1 = P_\infty, P_2 = P_{0b_2}, P_3 = P_{0b_3}, \ldots, P_{q+1} = P_{0b_{q+1}}$ be $q+1$ distinct $\mathbb{F}_{q^2}$-rational points on the curve X defined by $y^q + y = x^m$ where $m > 2$ is a divisor of $q+1$. Let $2 \leq r \leq q+1$ and $\boldsymbol{\alpha}, \boldsymbol{\beta} \in \mathbb{N}_0^r$. Assume that $\alpha_1 \geq 1$,*

$$\{\mathbf{u} \in \mathbb{N}_0^r : u_1 = \alpha_1, \mathbf{u} \preceq \boldsymbol{\alpha}\} \subseteq G(P_1, \ldots, P_r),$$

and

$$\left\{ \begin{array}{c} \boldsymbol{\beta} - \mathbf{a} - \mathbf{1} + \mathbf{e_1}, \\ \boldsymbol{\beta} - \mathbf{a} - \mathbf{1} + \mathbf{e_1} + \mathbf{e_k}, \\ \boldsymbol{\beta} - \mathbf{a} - \mathbf{1} + (m+1)\mathbf{e_1} \end{array} : \begin{array}{l} \mathbf{a} \in \mathbb{N}_0^r, a_1 = 0, 1 \leq k \leq r, \\ \sum_{i=2}^r a_i \leq 2g - 1 - \sum_{i=1}^r \alpha_i \end{array} \right\} \subseteq G(P_1, \ldots, P_r).$$

Set $D := Q_1 + \cdots + Q_n$, where $Q_1, \ldots, Q_n$ are distinct $\mathbb{F}$-rational points and no Q_i is in the support of G. If the r-point code $C_\Omega(D, G)$ is nontrivial, then the minimum distance of this code is at least $\deg G - (2g-2) + 2$.

Proof. By Theorem 4.1, the minimum distance of $C_\Omega(D, G)$ is at least $\deg G - 2g + 3$. Put $w = \deg G - 2g + 3$. If there exists a codeword of weight w, then there exists a differential $\eta \in \Omega(G - D)$ with exactly w simple poles $Q_1, \ldots, Q_w$. We have that $(\eta) \geq G - (Q_1 + \cdots + Q_w)$. Since $2g - 2 = \deg(\eta) = \deg G - w + 1$,

$$(\eta) = G - (Q_1 + \cdots + Q_w) + A,$$

where A is an $\mathbb{F}_{q^2}$-rational point and $A \neq Q_i$ for $1 \leq i \leq w$. Since $l(\sum_{i=1}^r \alpha_i P_i) = l((\alpha_1 - 1)P_1 + \sum_{i=2}^r \alpha_i P_i)$, there exists a rational function h with divisor

$$(h) = (\alpha_1 - 1)P_1 + \sum_{i=2}^r (\alpha_i + a_i)P_i - K + E,$$

where E is an effective divisor whose support does not contain any P_i and $0 \leq \sum_{i=2}^r a_i \leq 2g - 1 - (\sum_{i=1}^r \alpha_i)$ for each i, $2 \leq i \leq r$. Then

$$G - (Q_1 + \cdots + Q_w) + A = (\eta) \sim K \sim (\alpha_1 - 1)P_1 + \sum_{i=2}^r (\alpha_i + a_i)P_i + E$$

implies that there exists a rational function f with divisor

$$(f) = -\beta_1 P_1 - \left(\sum_{i=2}^r (\beta_i - a_i - 1)P_i \right) - A + (Q_1 + \cdots + Q_w) + E.$$

If A is in the support of E, then

$$(f) = -\beta_1 P_1 - \sum_{i=2}^{r}(\beta_i - a_i - 1)P_i + (Q_1 + \cdots + Q_w) + (E - A)$$

contradicting the assumption that $\boldsymbol{\beta} - \mathbf{a} - \mathbf{1} + \mathbf{e_1} \in G(P_1, \ldots, P_r)$. If $A = P_1$, then

$$(f) = -(\beta_1 + 1)P_1 - \sum_{i=2}^{r}(\beta_i - a_i - 1)P_i + (Q_1 + \cdots + Q_w) + E$$

contradicting the assumption that $\boldsymbol{\beta} - \mathbf{a} - \mathbf{1} + 2\mathbf{e_1} \in G(P_1, \ldots, P_r)$. If $A = P_k$ for $2 \leq k \leq r$, then

$$(f) = -\beta_1 P_1 - \sum_{\substack{i\,=\,2 \\ i\,\neq\,k}}^{r}(\beta_i - a_i - 1)P_i - (\beta_k - a_k)P_k + (Q_1 + \cdots + Q_w) + E$$

contradicting the assumption that $\boldsymbol{\beta} - \mathbf{a} - \mathbf{1} + \mathbf{e_1} + \mathbf{e_k} \in G(P_1, \ldots, P_r)$. Thus, $A = Q_j$ for some j, $w + 1 \leq j \leq n$. Then there exists a rational function $\tilde{f}$ on X with divisor $\left(\tilde{f}\right) = A' - mP_1$ where A' is an effective divisor whose support contains A (if $A = P_{ab}$, then one can take $\tilde{f} = y - b$). Once again a contradiction is reached as

$$\left(f\tilde{f}\right) = -(\beta_1 + m)P_1 - \sum_{i=2}^{r}(\beta_i - a_i - 1)P_i + (A' - A) + Q_1 + \cdots + Q_w + E.$$

Therefore, $C_\Omega(D, G)$ has no codeword of weight w. Hence, the minimum distance of $C_\Omega(D, G)$ is at least $w + 1 = \deg G - (2g - 2) + 2$. □

Next, we wish to compare r-point codes, $r \geq 2$, constructed using the Weierstrass gap set determined in Theorem 3.7 to other codes over the same field. The exact parameters of all one-point codes on the curve $y^q + y = x^m$ can be obtained from [10] or by applying the methods in [17], [4], and [19]. For reference purposes, we include Table 1 indicating the parameters of all one-point codes $C_\mathcal{L}(D', \alpha P_\infty)$ (equivalently, $C_\Omega(D', \alpha P_\infty)$) where D' is the sum of all $\mathbb{F}_{q^2}$-rational point other than P_∞. Note that the length of such a one-point code is $n' = q(m(q-1)+1)$. The dimension is denoted by k' and the minimum distance is denoted by d'.

Consider the r-point $[n, k, d]$ code $C_\Omega(D, G)$ on X with $2g - 2 < \deg G < n$. Then the dimension of $C_\Omega(D, G)$ is $k = n + g - 1 - \deg G$. If $\deg G < n - g - 1$, then $C_L(D', \alpha P_\infty)$ is the unique one-point code on X with dimension k, where $\alpha = k + g - 1$. Note that $C_L(D', \alpha P_\infty)$ has length $n' := n + r - 1$. From Table 1, we can see that if $n + r - 1 - \alpha \in H(P_\infty)$, then $C_L(D', \alpha P_\infty)$ is a $[n + r - 1, k, \deg G - (2g - 2) + r - 1]$ code. If $r = 2$ and $C_\Omega(D, G)$ satisfies the hypotheses of Theorem 4.1, then $C_\Omega(D, G)$ is a $[n, k, \geq \deg G - (2g - 2) + 2]$ code. Hence, this two-point code is shorter than the one-point code of the same dimension on X and corrects at least as many errors. Similarly, if $r = 3$, $C_\Omega(D, G)$ satisfies the hypotheses of Theorem 4.2, and $n + r - 1 - \alpha \in H(P_\infty)$, then $C_\Omega(D, G)$ has better parameters than the one-point code of the same dimension on X. Using these ideas, one can obtain the following corollary of Theorems 4.1 and 4.2.

Corollary 4.3. *Let X denote the quotient of the Hermitian curve over $\mathbb{F}_{q^2}$ defined by $y^q + y = x^m$ where $m > 2$ is a proper divisor of $q + 1$. Then there are r-point*

TABLE 1. Parameters of $C_{\mathcal{L}}(D', \alpha P_\infty)$

α	k'	d'
$0 \leq \alpha \leq 2g-1$	$\alpha + 1 - g$ $+ \mid H(P_\infty) \cap [0, 2g-2-\alpha] \mid$	$n' - \alpha + \min\{s \in \mathbb{N}_0 : \alpha - s \in H(P_\infty)\}$
$2g \leq \alpha \leq n'-2g$	$\alpha + 1 - g$	$n' - \alpha$
$n'-2g+1 \leq \alpha \leq n'-1$	$\alpha + 1 - g$	$n' - \alpha + \min\{s \in \mathbb{N}_0 : n' - \alpha + s \in H(P_\infty)\}$
$n' \leq \alpha \leq n'+2g-2$	$\alpha + 1 - g$ $+ \mid H(P_\infty) \cap [0, \alpha - n] \mid$	$\lfloor \frac{n-\alpha+2g-2}{\max\{q,m\}} \rfloor + 2$

codes on X with $r \geq 2$ that have better parameters than any comparable one-point code $C_{\mathcal{L}}(D, \alpha P_\infty)$ (or $C_\Omega(D, \alpha P_\infty)$) on the same curve.

Proof. We will prove the following statements:
(a) If $2g-2 < \delta < 4g-3$ and $\delta - (2g-2) + 1 \in H(P_\infty)$, then there is a two-point code $C_\Omega(D, G)$ on X with $\deg G = \delta$ and better parameters than the one-point code of the same dimension on X.
(b) If $2g-2 < \delta < \min\{(q-1-2c)m + 2, (q-c-3)m+1\} + (q-c-2)m + 1$ and $\delta - (2g-2) + 1 \in H(P_\infty)$, then there is a three-point code $C_\Omega(D, G)$ on X with $\deg G = \delta$ and better parameters than the one-point code of the same dimension on X.

Let $P_1 = P_\infty$, $P_2 = P_{0b_2}$, and $P_3 = P_{0b_3}$ be distinct $\mathbb{F}_{q^2}$-rational points on X. To obtain a two-point code as in (a), let $\boldsymbol{\alpha} = (1, 2g-2)$ and $\boldsymbol{\beta} = (1, \delta - (2g-2))$. Then Proposition 3.4 shows that the hypotheses of Theorem 4.1 are satisfied. Therefore, $C_\Omega(D, P_1 + (\delta-1)P_2)$ is an $[n, k, \geq \delta - (2g-2) + 1]$ code while the one-point code of dimension k is a $[n+1, k, \delta - (2g-2) + 1]$ code (since $\delta - (2g-2) + 1 \in H(P_\infty)$).

To obtain a three-point code as in (b), let $\boldsymbol{\alpha} = (1, 1, 2g-2-m) = (1, 1, (q-c-2)m)$ and $\boldsymbol{\beta} = (1, 1, \delta - (2g-2-m) - 1) = (1, 1, \delta - (q-c-m) - 1)$. Then Theorem 3.7 shows that the hypotheses of Theorem 4.2 are satisfied. Therefore, $C_\Omega(D, P_1 + P_2 + (\delta-2)P_2)$ is an $[n, k, \geq \delta - (2g-2) + 2]$ code while the one-point code of dimension k is a $[n+2, k, \delta - (2g-2) + 2]$ code (since $\delta - (2g-2) + 2 \in H(P_\infty)$). □

The proof the above corollary gives rise to many applications of Theorem 4.1 and Theorem 4.2.

Example 4.4. Let X denote the curve defined by $y^8 + y = x^3$ over $\mathbb{F}_{64}$. Then X has genus 7 and 177 $\mathbb{F}_{64}$-rational points. Hence, a two-point code on X has length $n := 175$ while a one-point code on X has length $n' := 176$. Let $\delta \in \{17, 19, 20, 22, 23\}$. Then Theorem 4.1 applies with $\boldsymbol{\alpha} = (1, 2g-2) = (1, 12)$ and $\boldsymbol{\beta} = (1, \delta - (2g-2)) = (1, \delta - 12)$ to give two-point codes $C_\Omega(D, P_\infty + (\delta-1)P_{00})$ with following parameters: $[175, 164, \geq 6]$, $[175, 162, \geq 8]$, $[175, 161, \geq 9]$, $[175, 159, \geq 11]$, and $[175, 158, \geq 12]$. For each choice of δ above, $\delta - (2g-2) + 1 = \delta - 11 \in H(P_\infty)$. Using Table 1, we see that one-point codes comparable (meaning of the same dimension) to those listed above have the following parameters: $[176, 164, 6]$, $[176, 162, 8]$, $[176, 161, 9]$, $[176, 159, 11]$, and $[176, 158, 12]$. Thus, in each of these cases, the two-point code has larger information rate (being shorter) than the comparable one-point code and at least the same error-correcting capability. We can also see that when $\delta = 20$, Theorem 4.2 applies with the choice of $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ given above. This shows that the code $C_\Omega(D, P_\infty + 16P_{00})$ is actually a $[175, 161, \geq 10]$ code. Sometimes, a different choice of $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are necessary to apply Theorem 4.2.

Next, we consider the three-point code $C_\Omega(D'', P_\infty + P_{00} + 14P_{01}$ on the same curve. Note that $P_\infty + P_{00} + 14P_{01} = (1+1-1)P_\infty + (1+1-1)P_{00} + (9+6-1)P_{01}$. According to Theorem 3.7 (and Example 3.8 in particular), we make take $\boldsymbol{\alpha} = (1,1,9)$ and $\boldsymbol{\beta} = (1,1,6)$ in Theorem 4.1. Then we conclude that $C_\Omega(D'', P_\infty + P_{00} + 14P_{01}$ is a $[174, 163, \geq 5]$ code. According to Table 1, the one-point code with dimension 163 is a $[176, 163, 6]$ code. Thus far, it is not clear how the one- and two-point codes compare. However, Theorem 4.2 also applies here so that the two-point code is actually a $[174, 163, \geq 6]$ code. This illustrates how more powerful results are needed when comparing r-point codes with one-point codes for larger values of r.

After considering two- and three-point codes in the previous corollary and example, it is natural to continue this line of reasoning for r-point codes where $r > 3$. In order to see that the minimum distances of such r-point codes rival that of one-point codes on the same curve, one needs results showing that given certain conditions the minimum distance of an r-point code is at least $r-1$ greater than its designed distance. For $r > 3$, the method of proof in Theorems 4.1 and 4.2 breaks down as r increases since it becomes necessary to consider all possible divisors of degree $r-1$ (in particular, the degree of the divisor A in the proof of Theorem 4.2 is $r-1$ which allows the possibility that A is a $\mathbb{F}_{(q^2)^{r-1}}$-rational point). In [9], the authors introduce another way to obtain such a result under much more restrictive conditions. This was generalized in [3]. For reference purposes, we record this below. An element $\boldsymbol{\alpha}$ of the Weierstrass gap set $G(P_1, \ldots, P_r)$ is called a pure gap of the r-tuple $(P_1, \ldots, P_r)$ if $\mathbf{n} \in G(P_1, \ldots, P_r)$ for all $\mathbf{n} \leq \boldsymbol{\alpha}$ with $n_i = \alpha_i$ for some i, $1 \leq i \leq r$.

Proposition 4.5. [9, Theorem 3.4] [3] *Let $G = \sum_{i=1}^{r} (\alpha_i + \beta_i - 1)P_i$ be a divisor on X supported by r distinct $\mathbb{F}$-rational points. Assume that $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are pure gaps of the r-tuple $(P_1, \ldots, P_r)$. Set $D := Q_1 + \cdots + Q_n$, where $Q_1, \ldots, Q_n$ are distinct $\mathbb{F}$-rational points and no Q_i is in the support of G. If the r-point code $C_\Omega(D, G)$ is nontrivial, then the minimum distance of this code is at least* $\deg G - (2g-2) + r$.

Example 4.6. Let X denote the curve defined by $y^8 + y = x^3$ over $\mathbb{F}_{64}$. Set $P_1 = P_\infty$, $P_2 = P_{00}$, $P_3 = P_{01}$ and $P_4 = P_{0\omega^9}$ where ω is a primitive element of $\mathbb{F}_{64}$ satisfying $\omega^6 + \omega^4 + \omega^3 + \omega + 1 = 0$. According to Theorem 3.7, $(1,1,1,7) \in \Gamma_4(P_1, P_2, P_3, P_4)$ which implies that $(1,1,1,7)$ is minimal in each of the sets $\{\mathbf{n} \in H(P_1, P_2, P_3, P_4) : n_i = 1\}$, $1 \leq i \leq 3$, and $\{\mathbf{n} \in H(P_1, P_2, P_3, P_4) : n_4 = 7\}$. We also know that $(0,0,0,5) \in G(P_1, P_2, P_3, P_4)$ since $5 \in H(P_4)$ by Proposition 3.3. It follows that $(1,1,1,5)$ is a pure gap of (P_1, P_2, P_3, P_4). Take $\boldsymbol{\alpha} = \boldsymbol{\beta} = (1,1,1,5)$ in Proposition 4.5 to obtain that the 4-point code $C_\Omega(D, P_1 + P_2 + P_3 + 9P_4)$ has minimum distance $d \geq 12 - 12 + 4 = 4$. Hence, $C_\Omega(D, P_1 + P_2 + P_3 + 9P_4)$ is a $[173, 167, \geq 4]$ code.

Clearly, the hypotheses in Proposition 4.5 are much more restrictive than those in Theorems 4.1 and 4.2. In [12], we provide a result more general than Proposition 4.5. Even so, the results stated in this section apply to a larger class of codes that those bounds found in [12].

In the next example, we compare codes constructed using the quotient of the Hermitian curve $y^q + y = x^m$ where m is a proper divisor of $q+1$ with one-point Hermitian codes over $\mathbb{F}_{q^2}$. The parameters of all one-point Hermitian codes were determined in a series of works ([17], [4], [19]). For these parameters, see Table 1.

TABLE 2. $C_\Omega(D,G)$ versus one-point Hermitian $C_{\mathcal{L}}(D',G')$ over $\mathbb{F}_{64}$

$\deg G$	$\frac{k}{n}$	$\frac{k'}{n'}$	$\frac{d}{n}$	$\frac{d'}{n'}$
18	*0.9314*	*0.9297*	*0.0400*	*0.0716*
19	*0.9257*	*0.9238*	*0.0457*	*0.0312*
20	*0.9200*	*0.9199*	*0.0517*	*0.0312*
21	*0.9143*	*0.9141*	*0.0517*	*0.0332*
22	*0.9086*	*0.9082*	*0.0629*	*0.0469*
23	*0.9029*	*0.9023*	*0.0686*	*0.0469*
24	*0.8971*	*0.8965*	*0.0743*	*0.0508*

Example 4.7. Let X denote the curve defined by $y^8+y=x^3$ over $\mathbb{F}_{64}$ and let X' denote the Hermitian curve over $\mathbb{F}_{64}$, which may be defined by $y^8+y=x^9$. Notice that X has genus 7 and 177 $\mathbb{F}_{64}$-rational points while X' has genus 28 and 513 $\mathbb{F}_{64}$-rational points. One way to compare codes on these two curves is to compare codes with comparable information rates.

Suppose $C_\Omega(D,G)$ is a two-point code on X and $12=2g-2<\deg G<177-2$. Then $C_\Omega(D,G)$ has length $n=175$, dimension $k=181-\deg G$, and minimum distance $d\geq \deg G-12$. We compare this code with the $[n',k',d']$ one-point code $C_{\mathcal{L}}(D',AQ_\infty)$ on X' where A is chosen so that the codes $C_\Omega(D,G)$ and $C_{\mathcal{L}}(D',AQ_\infty)$ have comparable information rates; that is, A is chosen so that $\frac{k'}{n'}\approx\frac{k}{n}$. To illustrate this, let $G=4P_\infty+14P_{00}$ be a divisor of X. Then Theorem 4.1 applies with $\boldsymbol{\alpha}=(1,12)$ and $\boldsymbol{\beta}=(4,3)$ to give that $C_\Omega(D,G)$ is a $[175,163,\geq 7]$ code. Next, we find the one-point Hermitian code over $\mathbb{F}_{64}$ with information rate approximately that of $C_\Omega(D,G)$. This is done by choosing the dimension k' of $C_{\mathcal{L}}(D',AQ_\infty)$ such that $k':=\lfloor\frac{512}{175}*163\rfloor=476$. This completely determines the code $C_{\mathcal{L}}(D',AQ_\infty)$. In fact, $A=503Q_\infty$ and $C_{\mathcal{L}}(D',AQ_\infty)$ is a $[512,476,9]$ code. It is easy to see that the relative distance of the two-point code is $\frac{d}{n}\geq 0.0400$ while the one-point code has relative distance $\frac{d'}{n'}=0.0176$. Table 4.7 give several other similar examples. Note that the divisor G is chosen so that Theorem 4.1 (or Theorem 4.2) applies.

APPENDIX A

The content of this appendix is the proof of Theorem 3.7.

Proof of Theorem 3.7. We begin by setting up some notation. Recall that the notation

$$\boldsymbol{\gamma}_{\mathbf{t},j}=((t_1-j)m+j,(t_2-j)m+j,\ldots,(t_r-j)m+j)$$

introduced in Definition 3.6 will only be used to describe vectors where $1\leq j\leq l-1$ and $j\leq t_i\leq q-1-j(c-1)$ for all $1\leq i\leq r$. For $2\leq r\leq q+1$, set

$$S_r:=\left\{\boldsymbol{\gamma}_{\mathbf{t},j}\in\mathbb{N}^r:\sum_{i=1}^r t_i=(m-j)c+r(j-1)\right\}.$$

For $2\leq r\leq q+1$, we will prove that $\tilde{\Gamma}_r=S_r$ by induction on r. According to Proposition 3.4,

$$\tilde{\Gamma}_2=\left\{\boldsymbol{\gamma}_{(t_1,t_2),j}\in\mathbb{N}^2:t_1+t_2=(m-j)c+2(j-1)\right\}=S_2,$$

which settles the case where $r = 2$. We now proceed by induction on $r \geq 3$. Assume that $\tilde{\Gamma}_i = S_i$ holds for all $2 \leq i \leq r-1$.

First, we claim that $S_r \subseteq \tilde{\Gamma}_r$. Let $\boldsymbol{\gamma}_{\mathbf{t},j} \in S_r$. Then

$$\left(\frac{x^{m-j}}{\prod_{i=2}^{r}(y-b_i)^{t_i-j+1}}\right)_\infty = \sum_{i=1}^{m}((t_i-j)m+j)P_i.$$

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

In order to show that $\boldsymbol{\gamma}_{\mathbf{t},j} \in \tilde{\Gamma}_r$, it suffices to prove that $\boldsymbol{\gamma}_{\mathbf{t},j}$ is minimal in $\{\mathbf{p} \in H_r : p_1 = (t_1-j)m+j\}$. Suppose $\boldsymbol{\gamma}_{\mathbf{t},j}$ is not minimal in

$$\{\mathbf{p} \in H_r : p_1 = (t_1-j)m+j\}.$$

Then there exists $\mathbf{u} \in H_r$ with $u_1 = (t_1-j)m+j$, $\mathbf{u} \preceq \boldsymbol{\gamma}_{\mathbf{t},j}$, and $\mathbf{u} \neq \boldsymbol{\gamma}_{\mathbf{t},j}$. Let $f \in \mathbb{F}_{q^2}(X)$ be such that $(f)_\infty = u_1P_1 + \cdots + u_rP_r$. Without loss of generality, we may assume that $u_r < (t_r-j)m+j$ as $\mathbf{u} \neq \boldsymbol{\gamma}_{\mathbf{t},j}$ gives $u_i < (t_i-j)m+j$ for some $2 \leq i \leq r$ and a similar argument holds if $2 \leq i \leq r-1$. Hence,

$$u_r = (t_r-j)m+j-k$$

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

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

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

$$\left(f(y-b_r)^{t_r-j}x^{j-k}\right)_\infty = ((t_1+t_r+(c-2)(j-k)-k-k)m+k)P_1+\sum_{i=2}^{r-1}\max\{u_i-(j-k),0\}P_i.$$

Therefore,

$$\mathbf{v} := ((t_1+t_r+(c-2)(j-k)-k-k)m+k, v_2, \ldots, v_{r-1}) \in H_{r-1},$$

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

$$\mathbf{w} := \boldsymbol{\gamma}_{(t_1+t_r+(c-2)(j-k)-k, t_2-j+1+k, t_3-j+k, \ldots, t_{r-1}-j+k), k}.$$

Clearly,

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

Note that

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

since $t_1+t_r+(c-2)(j-k)-k+t_2-j+1+k+\sum_{i=3}^{r-1}(t_i-j+k) = (m-k)c+(r-1)(k-1)$. By the induction hypothesis, $S_{r-1} = \tilde{\Gamma}_{r-1}$, and so

$$\mathbf{w} \in \tilde{\Gamma}_{r-1}.$$

By Lemma 3.1, $\mathbf{w}$ is minimal in the set $\{\mathbf{p} \in H_{r-1} : p_1 = (t_1+t_r+(c-2)(j-k)-k-k)m+k\}$. This leads to a contradiction as

$\mathbf{v} \in \{\mathbf{p} \in H_{r-1} : p_1 = (t_1+t_r+(c-2)(j-k)-k-k)m+k\}$,
$\mathbf{v} \preceq \mathbf{w}$, and
$\mathbf{v} \neq \mathbf{w}$.

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

$$\left(f(y-b_r)^{t_r-j}\right)_\infty = ((t_1+t_r-j-j)m+j)P_1 + \sum_{i=2}^{r-1}u_iP_i$$

which implies that

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

Note that there exists i, $2 \leq i \leq r-1$, such that $t_i < q-1-j(c-1)$ since otherwise $2j \leq t_1+t_r = -(r-3)(q+1-jc)+r-4+2j$ implies that $0 \leq -(r-3)(c(m-j)-1)-1$ contradicting the assumption that $r \geq 3$. We may assume that $i = 2$ as a similar argument holds in the case $2 < i \leq r-1$. Then set

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

Clearly,

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

Also note that

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

since $t_1 + t_r - j + t_2 + 1 + \sum_{i=3}^{r-1} t_i = (m-j)c + (r-1)(j-1)$. By the induction hypothesis, $S_{r-1} = \tilde{\Gamma}_{r-1}$, and so

$$\mathbf{w} \in \tilde{\Gamma}_{r-1}.$$

According to Lemma 3.1, $\mathbf{w}$ is minimal in $\{\mathbf{p} \in H_{r-1} : p_1 = (t_1+t_r-j-j)m+j\}$. This leads to a contradiction as

$$\begin{array}{l} \mathbf{v} \in \{\mathbf{p} \in H_{r-1} : p_1 = (t_1 + t_r - j - j)m + j\}, \\ \mathbf{v} \preceq \mathbf{w}, \text{ and} \\ \mathbf{v} \neq \mathbf{w}. \end{array}$$

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

$$S_r \subseteq \tilde{\Gamma}_r.$$

Next, we will show that $\tilde{\Gamma}_r \subseteq S_r$. Suppose not; that is, suppose that there exists $\mathbf{n} \in \tilde{\Gamma}_r \setminus S_r$. Then there exists $f \in \mathbb{F}_{q^2}(X)$ such that $(f)_\infty = n_1P_1 + \cdots + n_rP_r$. By Lemma 3.5,

$$\mathbf{n} \in \tilde{\Gamma}_r \subseteq G(P_1) \times G(P_2) \times \cdots \times G(P_r).$$

Thus,

$$\mathbf{n} = ((t_1 - j_1)m + j_1, (t_2 - j_2)m + j_2, \ldots, (t_r - j_r)m + j_r)$$

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

$$(f(y-b_r)^{t_r-j_r+1})_\infty = (n_1 + (t_r - j_r + 1)m)P_1 + \sum_{i=2}^{r-1} n_iP_i,$$

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

$$\mathbf{u} \preceq (n_1 + (t_r - j_r + 1)m, n_2, \ldots, n_{r-1})$$

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

$$\tilde{\mathbf{u}} = \boldsymbol{\gamma}_{(T_{i_1},\ldots,T_{i_k}),j'} \in S_k = \tilde{\Gamma}_k$$

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

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

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

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

we have that $m \mid (j' - j_2)$. This forces $j' = j_2$ (and consequently $T_2 = t_2$) as $1 \leq j', j_2 \leq l-1 \leq m-1$. As a result,

$$\tilde{\mathbf{u}} = \boldsymbol{\gamma}_{(T_1, T_2, T_{i_3}, \ldots, T_{i_k}), j_2},$$

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

$T_1 + T_2 + T_{i_3} + \cdots + T_{i_k} = (m - j_2)c + k(j_2 - 1)$, and $j_2 \leq T_{i_s} \leq q - 1 - j_2(c-1)$ for all $1 \leq s \leq k$. At this point, we separate the proof into two cases:

$$\begin{array}{ll} (1) & u_1 - (t_r - j_r + 1)m \geq 0 \\ (2) & u_1 - (t_r - j_r + 1)m < 0. \end{array}$$

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

$$\mathbf{v} := (u_1 - (t_r - j_r + 1)m, u_2, u_3, \ldots, u_{r-1}, (t_r - j_r + j_2 - j_2)m + j_2).$$

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

$$\tilde{\mathbf{v}} = \boldsymbol{\gamma}_{(T_1 - t_r + j_r - 1, T_2, T_{i_3}, \ldots, T_{i_k}, t_r - j_r + j_2), j_2}.$$

Since $T_1 - t_r + j_r - 1 + T_2 + (\sum_{s=3}^{k} T_{i_s}) + t_r - j_r + j_2 = (m - j_2)c + (k+1)(j_2 - 1)$, this establishes the claim that $\tilde{\mathbf{v}} \in S_{k+1}$. Since $S_{k+1} \subseteq \tilde{\Gamma}_{k+1}$, it follows that $\mathbf{v} \in \Gamma_r \subseteq H_r$. Now, $\mathbf{v} \preceq \mathbf{n}$ and $\mathbf{n} \in \tilde{\Gamma}_r$ force $\mathbf{n} = \mathbf{v}$ as otherwise $\mathbf{n}$ is not minimal in $\{\mathbf{p} \in H_r : p_2 = n_2\}$. Hence, $k+1 = r$ and $\mathbf{n} = \mathbf{v} = \tilde{\mathbf{v}} \in S_r$, which is a contradiction.

Case (2): Suppose that $u_1 - (t_r - j_r + 1)m < 0$. There are two subcases to consider:

$$\begin{array}{ll} (a) & j_1 < t_1 \\ (b) & j_1 = t_1. \end{array}$$

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

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

Notice that $\mathbf{v} \preceq \mathbf{n}$ and $\mathbf{v} \neq \mathbf{n}$ since $j_2 - m < 0 \leq j_1$, $u_i \leq n_i$ for $2 \leq i \leq r-1$, and $(T_1 - j_2)m + j_2 = u_1 < (t_r - j_r + 1)m$ implies that $(T_1 - t_1 + j_1 - j_2)m + j_2 \leq (t_r - j_r)m + j_r$ as $j_2 \leq j_r$. The fact that $j_1 < t_1$ gives $\tilde{\mathbf{v}} \in \mathbb{N}^{k+1}$. We claim that $\tilde{\mathbf{v}} \in S_{k+1}$. To see this, express $\tilde{\mathbf{v}}$ as

$$\tilde{\mathbf{v}} = \boldsymbol{\gamma}_{(t_1 - j_1 + j_2 - 1, T_2, T_{i_3}, \ldots, T_{i_k}, T_1 - t_1 + j_1), j_2}.$$

(In order to write $\tilde{\mathbf{v}}$ in this manner, it must be checked that $t_1 - j_1 + j_2 - 1 \leq q - 1 - j_2(c-1)$ 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 $t_1 - j_1 + j_2 - 1 \leq T_1 - 1 \leq q - 1 - j_2(c-1)$. If $j_2 > T_1 - t_1 + j_1$,

then $(T_1 - j_2)m \leq (t_1 - j_1)m + j_1 - j_2$, contradicting the fact that $u_1 > n_1$. Hence, $j_2 \leq T_1 - t_1 + j_1$.) It is easy to see that $t_1 - j_1 + j_2 - 1 + T_2 + T_{i_3} + \cdots + T_{i_k} + T_1 - t_1 + j_1 = (m - j_2)c + (k+1)(j_2 - 1)$, and so $\tilde{\mathbf{v}} \in S_{k+1} \subseteq \tilde{\Gamma}_{k+1}$. It follows that $\mathbf{v} \in H_r$ and so $\mathbf{v} \in \{\mathbf{p} \in H_r : p_2 = n_2\}$. This yields a contradiction as $\mathbf{n}$ is minimal in $\{\mathbf{p} \in H_r : p_2 = n_2\}$, concluding the proof in this subcase.

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

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

Then $\mathbf{v} \preceq \mathbf{n}$ and $\mathbf{v} \neq \mathbf{n}$ since $0 < n_1$, $u_i \leq n_i$ for $2 \leq i \leq r-1$, and $u_1 < (t_r - j_r + 1)m$ implies $T_1 - j_2 \leq t_r - j_r$ which means $(T_1 - j_2)m + j_2 \leq (t_r - j_r)m + j_r$ as $j_2 \leq j_r$. It is easy to see that $\tilde{\mathbf{v}} \in S_k$ as $\sum_{s=1}^{k} T_{i_s} = (m - j_2)c + k(j_2 - 1)$ and $j_2 \leq T_{i_s} \leq q - 1 - j(c-1)$ for all $1 \leq s \leq k$. As before, it follows that $\mathbf{v} \in H_r$ and $\mathbf{v} \in \{\mathbf{p} \in H_r : p_2 = n_2\}$. Since $\mathbf{v} \neq \mathbf{n}$, this contradicts the minimality of $\mathbf{n}$ in the set $\{\mathbf{p} \in H_r : p_2 = n_2\}$, 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, $\tilde{\Gamma}_r \setminus S_r = \emptyset$. This establishes that $\tilde{\Gamma}_r \subseteq S_r$, concluding the proof that $\tilde{\Gamma}_r = S_r$.

Now suppose that $q + 1 - c < r \leq q + 1$. If $\boldsymbol{\gamma}_{\mathbf{t},j} \in \tilde{\Gamma}_r$, then

$$rj \leq \sum_{i=1}^{r} t_i = (m - j)c + r(j-1) \leq (q + 1 - c)j$$

which is a contradiction. Therefore, $\tilde{\Gamma}_r = \emptyset$. □

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*, to appear in Des. Codes and Cryptog.

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

[6] V. D. Goppa, *Algebraico-geometric codes*, Math. USSR-Izv. **21** (1983), 75–91.

[7] V. D. Goppa, *Geometry and Codes*, Kluwer, 1988.

[8] M. Homma, *The Weierstrass semigroup of a pair of points on a curve*, Arch. Math. **67** (1996), 337–348.

[9] M. Homma and S. J. Kim, *Goppa codes with Weierstrass pairs*, J. Pure Appl. Algebra **162** (2001), 273–290.

[10] T. Johnsen, S. Manshadi, and N. Monzavi, *A determination of the parameters of a large class of Goppa codes*, IEEE Trans. Inform. Theory **40** no. 5 (1994), 1678–1681.

[11] S. J. Kim, *On the index of the Weierstrass semigroup of a pair of points on a curve*, Arch. Math. **62** (1994), 73–82.

[12] H. Maharaj, G. L. Matthews, and G. Pirsic, Riemann-Roch spaces of the Hermitian function field with applications to algebraic geometry codes and low-discrepancy sequences, in review.

[13] G. L. Matthews, *Codes from the Suzuki function field*, in review.

[14] G. L. Matthews, *Weierstrass pairs and minimum distance of Goppa codes*, Des. Codes and Cryptog. **22** (2001), 107–121.

[15] G. L. Matthews, *The Weierstrass semigroup of an m-tuple of collinear points on a Hermitian curve*, to appear in the proceedings of the Seventh International Conference on Finite Fields and Applications (Toulouse, 2003).

[16] F. K. Schmidt, *Zur arithmetischen Theorie der algebraischen Funktionen II. Allgemeine Theorie der Weierstrasspunkte*, Math. Z. **45** (1939), 75–96.
[17] H. Stichtenoth, *A note on Hermitian codes*, IEEE Trans. Inform. Theory **33** (1988), 1345–1348.
[18] C. P. Xing and H. Chen, *Improvements on parameters of one-point AG codes from Hermitian codes*, IEEE Trans. Inform. Theory **48** no. 2 (2002), 535–537.
[19] K. Yang and P. V. Kumar, *On the true minimum distance of Hermitian codes*, Coding Theory and Algebraic Geometry, Proceedings, Luminy, 1991, Lecture Notes in Mathematics **1518**, Springer-Verlag, 1992, 99–107.