WEIERSTRASS PAIRS AND MINIMUM DISTANCE OF GOPPA CODES

GRETCHEN L. MATTHEWS
DEPARTMENT OF MATHEMATICS
UNIVERSITY OF TENNESSEE
KNOXVILLE, TN 37996
MATTHEWS@MATH.UTK.EDU

Abstract. We prove that elements of the Weierstrass gap set of a pair of points may be used to define a geometric Goppa code which has minimum distance greater than the usual lower bound. We determine the Weierstrass gap set of a pair of any two Weierstrass points on a Hermitian curve and use this to increase the lower bound on the minimum distance of particular codes defined using a linear combination of the two points.

1. Introduction

Goppa [4, 5] constructed linear codes from two divisors G and D on a curve, and using the Riemann-Roch Theorem, obtained estimates of the dimension and minimum distance of these codes. In particular, he gave a lower bound for the minimum distance. In [2] Garcia, Kim, and Lax showed that if G is taken to be a multiple of a point P, the structure of the gap sequence at P may allow one to give a better lower bound on the minimum distance. Arbarello, Cornalba, Griffiths, and Harris [1] generalized the notion of the gap sequence at a point to the Weierstrass gap set of a pair of points on a curve. This was expounded upon by Kim [7] and Homma [6]. In this paper, we show that if G is an effective divisor that is a linear combination of two points P_1 and P_2, then knowledge of the Weierstrass gap set of the pair (P_1, P_2) may allow one to conclude that the minimum distance is greater than Goppa's lower bound. In some cases, this gives codes with better parameters (length, dimension, and minimum distance) than those considered by Garcia, Kim, and Lax.

This paper is organized as follows. Section 2 provides basic definitions and properties of geometric Goppa codes and those of the Weierstrass semigroup of a pair of points. Section 3 contains our main result relating this semigroup to codes on arbitrary curves. In Section 4 we compute the Weierstrass gap set of a pair of Weierstrass points on a Hermitian curve, and using this we obtain results specialized to codes on Hermitian curves in Section 5. Section 6 contains examples illustrating our theorems.

Date: June 23, 1999.
Key words and phrases. Weierstrass pair, Weierstrass point, Hermitian code.
These results appear in the author's LSU doctoral dissertation.

2. Preliminaries

Let X be a smooth projective absolutely irreducible curve of genus $g > 1$ over $\mathbb{F}_q$. For a divisor D on X defined over $\mathbb{F}_q$, let $L(D)$ denote the set of rational functions f on X defined over $\mathbb{F}_q$ with divisor $(f) \geq -D$ together with the zero function and let $\Omega(D)$ denote the set of rational differentials η on X defined over $\mathbb{F}_q$ with divisor $(\eta) \geq D$ together with the zero differential. Both $L(D)$ and $\Omega(D)$ are finite dimensional $\mathbb{F}_q$-vector spaces; let $l(D)$ and $i(D)$ denote their respective dimensions over $\mathbb{F}_q$. The Riemann-Roch Theorem states that

$$\begin{aligned} l(D) &= \deg\, D + 1 - g + i(D) \\ &= \deg\, D + 1 - g + l(K - D), \end{aligned}$$

where K is any canonical divisor on X. 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 $(f)_\infty$. Two divisors D_1 and D_2 are linearly equivalent, denoted $D_1 \sim D_2$, if $D_1 - D_2 = (f)$ for some rational function f.

Let G be a divisor on X defined over $\mathbb{F}_q$ and let $D = Q_1 + \cdots + Q_n$ be another divisor on X where $Q_1, \ldots, Q_n$ are distinct $\mathbb{F}_q$-rational points, each not belonging to the support of G. The geometric Goppa codes $C_L(D, G)$ and $C_\Omega(D, G)$ are constructed as follows. We give Stichtenoth [8] as a general reference. The code $C_L(D, G)$ is the image of the linear map $\phi : L(G) \to \mathbb{F}_q^n$ defined by

$$f \mapsto (f(Q_1), f(Q_2), \ldots, f(Q_n)).$$

If $\deg G < n$, then this code has dimension $l(G) \geq \deg G + 1 - g$ and minimum distance at least $n - \deg G$. The code $C_\Omega(D, G)$ is the image of the linear map $\phi^* : \Omega(G - D) \to \mathbb{F}_q^n$ defined by

$$\eta \mapsto (res_{Q_1}(\eta), res_{Q_2}(\eta), \ldots, res_{Q_n}(\eta)).$$

If $\deg G > 2g - 2$, then this code has dimension $i(G - D) = l(K + D - G) \geq n - \deg G + g - 1$, where K is a canonical divisor, and minimum distance at least $\deg G - (2g - 2)$. The codes $C_L(D, G)$ and $C_\Omega(D, G)$ are dual codes. If $G = mP$ for some $\mathbb{F}_q$-rational point P, $m \in \mathbb{N}$, and D is the sum of all the other $\mathbb{F}_q$-rational points on X, we will refer to $C_L(D, G)$ and $C_\Omega(D, G)$ as one-point codes. If $G = \alpha_1 P_1 + \alpha_2 P_2$ for distinct $\mathbb{F}_q$-rational points P_1 and P_2, $\alpha_1, \alpha_2 \in \mathbb{N}$, and D is the sum of all the other $\mathbb{F}_q$-rational points on X, we will refer to $C_L(D, G)$ and $C_\Omega(D, G)$ as two-point codes. Note that a two-point code has length one less than that of a one-point code on the same curve.

Let $\mathbb{F}_q(X)$ denote the field of rational functions on X defined over $\mathbb{F}_q$. For $\mathbb{F}_q$-rational points P_1 and P_2, one defines the Weierstrass semigroup of the point P_1 by

$$H(P_1) = \{\alpha \in \mathbb{N}_0 : \exists f \in \mathbb{F}_q(X) \text{ with } (f)_\infty = \alpha P_1\}$$

and the Weierstrass semigroup of a pair of points (P_1, P_2) by

$$H(P_1, P_2) = \{(\alpha_1, \alpha_2) \in \mathbb{N}_0^2 : \exists f \in \mathbb{F}_q(X) \text{ with } (f)_\infty = \alpha_1 P_1 + \alpha_2 P_2\},$$

where $\mathbb{N}_0$ denotes the set of nonnegative integers. Define the Weierstrass gap sets $G(P_1)$ and $G(P_1, P_2)$ by

$$G(P_1) = \mathbb{N}_0 \setminus H(P_1)$$

and

$$G(P_1, P_2) = \mathbb{N}_0^2 \setminus H(P_1, P_2).$$

These two sets differ in that for any $\mathbb{F}_q$-rational point P_1, $|G(P_1)| = g$, but $|G(P_1, P_2)|$ depends on the choice of points P_1 and P_2 [1]. Since

$$H(P_1, P_1) = \{(\alpha_1, \alpha_2) \in \mathbb{N}_0^2 : \alpha_1 + \alpha_2 \in H(P_1)\}$$

depends only on $H(P_1)$, in the following we assume $P_1 \neq P_2$.

We state a useful characterization of the elements of $H(P_1, P_2)$, which appears in [7]:

Lemma 2.1. *For $(\alpha_1, \alpha_2) \in \mathbb{N}^2$, the following are equivalent:*
(i) $(\alpha_1, \alpha_2) \in H(P_1, P_2)$.
(ii) $l(\alpha_1 P_1 + \alpha_2 P_2) = l((\alpha_1 - 1)P_1 + \alpha_2 P_2) + 1 = l(\alpha_1 P_1 + (\alpha_2 - 1)P_2) + 1$.

We will often make use of the following lemma, also from [7]:

Lemma 2.2. *Let $\alpha_1 \geq 1$. Then $l(\alpha_1 P_1 + \alpha_2 P_2) = l((\alpha_1 - 1)P_1 + \alpha_2 P_2) + 1$ if and only if there exists α, $0 \leq \alpha \leq \alpha_2$, such that $(\alpha_1, \alpha) \in H(P_1, P_2)$.*

Suppose $(\alpha_1, \alpha_2) \in G(P_1, P_2)$. Then by Lemma 2.1 , either $l(\alpha_1 P_1 + \alpha_2 P_2) = l((\alpha_1 - 1)P_1 + \alpha_2 P_2)$ or $l(\alpha_1 P_1 + \alpha_2 P_2) = l(\alpha_1 P_1 + (\alpha_2 - 1)P_2)$. Thus, if $\alpha_1 \geq 1$, there is no loss of generality in assuming that $l(\alpha_1 P_1 + \alpha_2 P_2) = l((\alpha_1 - 1)P_1 + \alpha_2 P_2)$. Note that by Lemma 2.2 this is the case exactly when $(\alpha_1, \alpha) \in G(P_1, P_2)$ for all α, $0 \leq \alpha \leq \alpha_2$.

3. Main Theorem for Codes on Arbitrary Curves

In this section, we relate the Weierstrass gap set of a pair of points to the minimum distance of a corresponding two-point code. This result is analogous to Theorem 1 of Garcia, Kim, and Lax [2].

Theorem 3.1. *Assume that $(\alpha_1, \alpha_2) \in G(P_1, P_2)$ with $\alpha_1 \geq 1$ and $l(\alpha_1 P_1 + \alpha_2 P_2) = l((\alpha_1 - 1)P_1 + \alpha_2 P_2)$. Suppose $(\gamma_1, \gamma_2 - t - 1) \in G(P_1, P_2)$ for all t, $0 \leq t \leq \min\{\gamma_2 - 1, 2g - 1 - (\alpha_1 + \alpha_2)\}$. Set $G = (\alpha_1 + \gamma_1 - 1)P_1 + (\alpha_2 + \gamma_2 - 1)P_2$, and let $D = Q_1 + \cdots + Q_n$, where the Q_i are distinct $\mathbb{F}_q$-rational points, each not belonging to the support of G. If the dimension of $C_\Omega(D, G)$ is positive, then the minimum distance of this code is at least* $\deg G - 2g + 3$.

Proof. Proof Put $w = \deg G - 2g + 2$. 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 then have $(\eta) \geq G - (Q_1 + \cdots + Q_w)$. Hence, $2g - 2 = \deg(\eta) \geq \deg G - w = 2g - 2$. It follows that

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

Since $l(\alpha_1 P_1 + \alpha_2 P_2) = l((\alpha_1 - 1)P_1 + \alpha_2 P_2)$, by the Riemann-Roch Theorem, there exists a rational function

$$h \in L(K - ((\alpha_1 - 1)P_1 + \alpha_2 P_2)) \backslash L(K - (\alpha_1 P_1 + \alpha_2 P_2))$$

for any canonical divisor K on X. Thus, $(h) = (\alpha_1 - 1)P_1 + \alpha_2 P_2 - K + E$, where E is an effective divisor of degree $2g - 1 - (\alpha_1 + \alpha_2)$ with P_1 not contained in its support. Write $E = E' + tP_2$, where E' is an effective divisor whose support does not contain P_2 (so $0 \leq t \leq \deg E = 2g - 1 - (\alpha_1 + \alpha_2)$). Then we can express the divisor of h as

$$(h) = (\alpha_1 - 1)P_1 + (\alpha_2 + t)P_2 - K + E'.$$

Now

$$G - (Q_1 + \cdots + Q_w) = (\eta) \sim K \sim (\alpha_1 - 1)P_1 + (\alpha_2 + t)P_2 + E'.$$

It follows that there is a rational function f with divisor

$$(f) = -\gamma_1 P_1 - (\gamma_2 - t - 1)P_2 + (Q_1 + \cdots + Q_w) + E'.$$

If $t \leq \gamma_2 - 1$, then f has pole divisor $(f)_\infty = \gamma_1 P_1 + (\gamma_2 - t - 1)P_2$, contradicting the fact that $(\gamma_1, \gamma_2 - t - 1) \in G(P_1, P_2)$. Otherwise, f has pole divisor $(f)_\infty = \gamma_1 P_1$, which is a contradiction as γ_1 is a gap at P_1. □

In [10], Yang and Kumar give the exact minimum distance for one-point codes on Hermitian curves. We can compare two-point codes to one-point codes on the same curve with the same dimension. If a two-point code has minimum distance at least that of a one-point code (of the same dimension), then the two-point code has better parameters (having shorter length). For codes on a Hermitian curve, we can see when Theorem 3.1 allows one to conclude that a two-point code has better parameters than any associated one-point code.

Proposition 3.2. *Consider a q^2-ary two-point code $C_\Omega(D, G)$ on the Hermitian curve $y^q + y = x^{q+1}$ satisfying the hypotheses of Theorem 3.1. If* $\deg G = 2g + q^2 - aq - b - 3$, $1 \leq a < b \leq q - 1$, *then this two-point code has minimum distance at least that of the one-point code $C_\Omega(D', m'P_\infty)$ on the same curve with the same dimension as $C_\Omega(D, G)$. Also, given any number $r = 2g + q^2 - aq - b - 3$, $1 \leq a < b \leq q - 1$, there is a two-point code $C_\Omega(D, G)$ on this Hermitian curve satisfying the hypotheses of Theorem 3.1 such that the degree of the divisor G is r.*

Proof. Proof Suppose $\deg G = 2g + q^2 - aq - b - 3$, $1 \leq a < b \leq q - 1$. Since $2g - 2 < \deg G < n$, where n is the degree of the divisor D, the dimension of $C_\Omega(D, G)$ is $i(G - D) = q^3 - q^2 + aq + b - g + 1$. By Theorem 3.1, the minimum distance of $C_\Omega(D, G)$ is at least $q^2 - aq - b$.

Let $m' = 2q^2 - (a+1)q - b - 2$. Consider the one-point code $C_\Omega(D', m'P_\infty)$. Then $C_\Omega(D', m'P_\infty)$ has dimension $k' = q^3 - q^2 + aq + b - g + 1$ and minimum distance $d' = q^2 - aq - b$ [10]. Therefore, $C_\Omega(D, G)$ is a $[q^3 - 1, q^3 - q^2 + aq + b - g + 1, \geq q^2 - aq - b]$ code and $C_\Omega(D', m'P_\infty)$ is a $[q^3, q^3 - q^2 + aq + b - g + 1, q^2 - aq - b]$ code. Note that by Corollary 1 of [10], the minimum distance d' uniquely determines k', so there is no one-point code with minimum distance d' and dimension larger than k'.

The proof of the last statement is deferred to Section 4 as we will need more information about the structure of the gap set of a pair of points on a Hermitian curve to conclude this. □

Note that the numbers $2g + q^2 - aq - b - 3$, $1 \leq a < b \leq q - 1$, form a "triangle" with legs of length $q - 2$:

$$\begin{array}{ccccc} 2g+q-2, & & & & \\ 2g+2q-2, & 2g+2q-1, & & & \\ 2g+3q-2, & 2g+3q-1, & 2g+3q, & & \\ \vdots & \vdots & \ddots & & \\ 2g+(q-2)q-2, & 2g+(q-2)q-1, & \ldots, & 2g+(q-2)q+q-5. & \end{array}$$

Remark 3.3. Let $C_\Omega(D, G)$ be a two-point code on the curve $y^q + y = x^{q+1}$ over $\mathbb{F}_{q^2}$ that satisfies the hypotheses of Theorem 3.1. Then, by Theorem 3.1, $C_\Omega(D, G)$ is a $[q^3 - 1, k, \geq \deg G - 2g + 3]$ code, where k denotes the dimension of the code. Suppose $C_\Omega(D', m'P_\infty)$ is a one-point code of dimension k on the same curve. Let d'

denote the minimum distance of this one-point code. Then $\deg G - 2g + 3 \geq d'$ only if the degree of G is of the form given in Proposition 3.2 or $\deg G = 2g + q^2 - aq - 3$, with $0 \leq a \leq q-1$. However, in the latter case, there is another one-point code with minimum distance d' and dimension greater than k.

4. Computation of $G(P_1, P_2)$ on a Hermitian Curve

In this section we determine the Weierstrass gap set of a pair of any two distinct Weierstrass points on a Hermitian curve. It is well known that the Weierstrass points of the Hermitian curve $y^q + y = x^{q+1}$ over $\mathbb{F}_{q^2}$ are exactly the $\mathbb{F}_{q^2}$-rational points. We will need some results of Kim [7].

Lemma 4.1. *If $(\alpha_1, \alpha_2), (\alpha_1', \alpha_2') \in H(P_1, P_2)$ with $\alpha_1 \geq \alpha_1'$ and $\alpha_2 \leq \alpha_2'$, then $(\alpha_1, \alpha_2') \in H(P_1, P_2)$.*

Definition 4.2. *For a gap α_1 at P_1, let $\beta_{\alpha_1} = \min\{\alpha_2 : (\alpha_1, \alpha_2) \in H(P_1, P_2)\}$.*

Lemma 4.3. *For a gap α_1 at P_1, $\alpha_1 = \min\{\alpha : (\alpha, \beta_{\alpha_1}) \in H(P_1, P_2)\}$. Also, $\{\beta_{\alpha_1} : \alpha_1 \in G(P_1)\} = G(P_2)$.*

Keeping this notation, we have

Theorem 4.4. *For any two distinct Weierstrass points P_1 and P_2 on the Hermitian curve $y^q + y = x^{q+1}$ over $\mathbb{F}_{q^2}$,*

$$\beta_{(t-j)(q+1)+j} = (q-t-1)(q+1) + j$$

for $1 \leq j \leq t \leq q-1$.

Proof. Proof Let $P_1 = P_{00}$ and $P_2 = P_\infty$ be the point at infinity, where P_{ab} denotes the common zero of $x - a$ and $y - b$. The divisors of x and y are given by

$$(x) = \sum_{\beta^q + \beta = 0} P_{0\beta} - qP_\infty \qquad \text{and} \qquad (y) = (q+1)(P_{00} - P_\infty).$$

It is well known that the gap sequence at P_1 (and at P_2) is

$$\begin{array}{ccccccc} 1 & & 2 & & \dots & q-2 & q-1 \\ (q+1)+1 & & (q+1)+2 & & \dots & (q+1)+(q-2) & \\ \vdots & & \vdots & & \iddots & & \\ (q-3)(q+1)+1 & & (q-3)(q+1)+2 & & & & \\ (q-2)(q+1)+1 & & & & & & \end{array} \tag{1}$$

Consider the diagonals in (1) running from the bottom left to the upper right (i.e. in the direction of $\nearrow$). Label these diagonals from 1 to $q-1$ starting at the upper left corner. Label the columns (resp. rows) of (1) from left to right (resp. top to bottom) starting with 1. Then, for a fixed t, $1 \leq j \leq t \leq q-1$, $(t-j)(q+1)+j$ is the number on the t^{th} diagonal in the j^{th} column.

For $1 \leq j \leq t \leq q-1$,

$$\left(\frac{x^{q-j+1}}{y^{t-j+1}}\right)_\infty = ((t-j)(q+1)+j)P_1 + ((q-t-1)(q+1)+j)P_2.$$

Therefore, $((t-j)(q+1)+j, (q-t-1)(q+1)+j) \in H(P_1, P_2)$. To see that this gives the β_α as claimed, start with $t = q-1$ and $1 \leq j \leq q-1$. This gives $((q-1-j)(q+1)+j, j) \in H(P_1, P_2)$ for $1 \leq j \leq q-1$. Hence, $\beta_{(q-1-j)(q+1)+j} = j$ for $1 \leq j \leq q-1$, which gives β_α for all gaps α at P_1 on the $(q-1)^{th}$ diagonal

in (1). Now let $t = q-2$ and $1 \leq j \leq q-2$ to get $\beta_{(q-2-j)(q+1)+j} = (q+1)+j$ for $1 \leq j \leq q-2$ (which gives β_α for all gaps α at P_1 on the $(q-2)^{th}$ diagonal of (1). Continuing in this manner, when $t = q-i$ and $1 \leq j \leq q-i$, we get $\beta_{(q-i-j)(q+1)+j} = (i-1)(q+1)+j$ for $1 \leq j \leq q-i$ (which gives β_α for all gaps α at P_1 on the $(q-i)^{th}$ diagonal of (1)). Finally, when $t = j = 1$, we get $\beta_1 = (q-2)(q+1)+1 = 2g-1$ and the theorem holds for $P_1 = P_{00}$ and $P_2 = P_\infty$.

Suppose $P_1 = P_{ab}$ with $(a,b) \neq (0,0)$ and $P_2 = P_\infty$. There exists an automorphism φ that fixes P_∞ and sends P_{ab} to P_{00} [9]. Then we can use the rational function $\frac{x^{q-j+1}}{y^{t-j+1}} \circ \varphi$ to compute the β_α as before.

Now suppose $P_1 = P_{ab}$ and $P_2 = P_{cd}$, where $(a,b) \neq (c,d)$. There exists an automorphism φ that leaves P_{ab} fixed and sends P_{cd} to P_∞ (namely, the composition $\varphi_1 \circ \varphi_2$, where φ_2 is an automorphism that sends P_{cd} to P_∞ and φ_1 is an automorphism that takes $\varphi_2(P_{ab})$ to P_{ab} and fixes P_∞) [9]. Then, as before, we get a rational function that gives rise to the β_α. □

To see what Theorem 4.4 means in terms of (1), we do the following. Make a new list (2) where the entry in the j^{th} column of row i of (1) is the entry in the j^{th} column and $(q-i)^{th}$ diagonal of (2):

$$
\begin{array}{cccccc}
 & (q-2)(q+1)+1 & (q-3)(q+1)+2 & \dots & (q+1)+(q-2) & q-1 \\
 & (q-3)(q+1)+1 & (q-4)(q+1)+2 & \dots & q-2 & \\
(2) & \vdots & \vdots & \iddots & & \\
 & (q+1)+1 & 2 & & & \\
 & 1 & & & &
\end{array}
$$

Note that the $(q-i)^{th}$ diagonal of (2) is the i^{th} row of (1). Now under each gap α at P_1 we want to write β_α. To do this, beginning with row 1, write the i^{th} row of (2) directly beneath the i^{th} row of (1):

$$
\begin{array}{cccccc}
 & 1 & 2 & \dots & q-2 & q-1 \\
 & (q-2)(q+1)+1 & (q-3)(q+1)+2 & \dots & (q+1)+(q-2) & q-1 \\
 & & & & & \\
 & (q+1)+1 & (q+1)+2 & \dots & (q+1)+(q-2) & \\
 & (q-3)(q+1)+1 & (q-4)(q+1)+2 & \dots & q-2 & \\
 & & & & & \\
(3) & \vdots & \vdots & \iddots & & \\
 & (q-3)(q+1)+1 & (q-3)(q+1)+2 & & & \\
 & (q+1)+1 & 2 & & & \\
 & & & & & \\
 & (q-2)(q+1)+1 & & & & \\
 & 1 & & & &
\end{array}
$$

Thus, if α is on the t^{th} diagonal in the j^{th} column of (1), i.e. $\alpha = (t-j)(q+1)+j$, then β_α is the number in (1) on the $(q-t+j-1)^{th}$ diagonal in the j^{th} column.

We can now prove the last statement of Propostion 3.2.

Proof. Proof Let $r = 2g+q^2-aq-b-3$, $1 \leq a < b \leq q-1$. Take $(\alpha_1, \alpha_2) = (1, 2g-2)$ and $(\gamma_1, \gamma_2) = (1, q^2-aq-b-1)$ in Theorem 3.1. By Theorem 4.4,

$\beta_1 = 2g-1$. Then $(1, 2g-2), (1, q^2-aq-b-2) \in G(P_1, P_2)$ and by Lemma 2.2, $l(P_1 + (2g-2)P_2) = l((2g-2)P_2)$. □

Knowing β_α for each gap α at P_1 allows us to compute $|G(P_1, P_2)|$ for any two distinct Weierstrass points P_1 and P_2 on a Hermitian curve. We will use the following result of Homma [6]:

Lemma 4.5. *Let P_1 and P_2 be any two distinct points on a smooth curve of genus $g > 1$. Then*

$$|G(P_1, P_2)| = \sum_{\alpha_1 \in G(P_1)} \alpha_1 + \sum_{\alpha_2 \in G(P_2)} \alpha_2 - r(P_1, P_2),$$

where $r(P_1, P_2) = |\{(\alpha_1, \alpha_1{}') \in G(P_1)^2 : \alpha_1 < \alpha_1{}' \text{ and } \beta_{\alpha_1} > \beta_{\alpha_1{}'}\}|$.

Theorem 4.6. *For any two distinct Weierstrass points P_1 and P_2 on the Hermitian curve $y^q + y = x^{q+1}$ over $\mathbb{F}_{q^2}$,*

$$|G(P_1, P_2)| = \frac{q}{12}(3q^3 - 4q^2 + 3q - 2).$$

Proof. Proof The sum of all the gaps at P_1 (equivalently, the sum of all the gaps at P_2) is

$$\begin{aligned}\sum_{\alpha_1 \in G(P_1)} \alpha_1 &= \sum_{t=1}^{q-1} \sum_{j=1}^{t} (q-t-1)(q+1) + j \\ &= \sum_{t=1}^{q-1} tq^2 - t^2 q - t^2 - t + \frac{t(t+1)}{2} \\ &= \frac{1}{6}(q^4 - q^3 - q^2 + q).\end{aligned}$$

Next we compute $r(P_1, P_2)$. Fix $1 \le j \le t \le q-1$. We need to count all pairs (t', j') such that

$$(t-j)(q+1) + j < (t'-j')(q+1) + j' \tag{4}$$

and

$$\beta_{(t-j)(q+1)+j} > \beta_{(t'-j')(q+1)+j'}.$$

Note that $\beta_{(t-j)(q+1)+j} > \beta_{(t'-j')(q+1)+j'}$ if and only if

$$(t'-t)(q+1) > j' - j. \tag{5}$$

First consider the case $t = t'$. Since $(t'-t)(q+1) = 0$, in order to satisfy (5), we must have $j > j'$. It is easy to see that all pairs with $t = t'$ and $j > j'$ satisfy both (4) and (5) and there are $t - j$ such pairs.

Now suppose $t > t'$. Then $(t'-t)(q+1) < 0$. Hence, to satisfy (5), j' must satisfy $j' < j$. However, $j' - j \ge -q+2$ (since $1 \le j, j' \le q-1$) and $(t'-t)(q+1) \le -q^2 - q$ (since $1 \le t, t' \le q-1$) imply that (5) fails.

The only case left to consider is $t' > t$. Here, (5) always holds since $j' - j \le q-2 < (t'-t)(q+1)$. If $j' \le j$, then $tq + t - jq < t'q + t' - j'q$ and so (4) holds. If $j' \ge j$, then (4) holds only in the case $t - j < t' - j'$. The number of pairs with $t' > t$ satisfying (4) and (5) is $\sum_{i=t+1}^{q-1} i - (t-j)(q-1-t)$.

Thus,

$$\begin{aligned}
r(P_1,P_2) &= \sum_{t=1}^{q-1}\sum_{j=1}^{t}(t-j+\sum_{i=t+1}^{q-1} i-(t-j)(q-1-t)) \\
&= \sum_{t=1}^{q-1}\sum_{j=1}^{t} t-j+\frac{q(q-1)}{2}-\frac{t(t+1)}{2}-tq+t+t^2+jq-j-jt \\
&= \sum_{t=1}^{q-1}\sum_{j=1}^{t} \frac{q^2}{2}-\frac{q}{2}-\frac{t^2}{2}-\frac{t}{2}-tq+2t+t^2+jq-2j-jt \\
&= \sum_{t=1}^{q-1} t(\frac{q^2}{2}-1)+t^2(\frac{-q}{2}) \\
&= (\frac{q^2}{2}-1)(\frac{q(q-1)}{2})-\frac{q}{2}(\frac{q(q-1)(2q-1)}{6}) \\
&= \frac{q}{12}(q^3-7q+6).
\end{aligned}$$

Therefore,

$$\begin{aligned}
|G(P_1,P_2)| &= \sum_{\alpha_1\in G(P_1)} \alpha_1 \ + \sum_{\alpha_2\in G(P_2)} \alpha_2 \ - r(P_1,P_2) \\
&= \frac{1}{3}(q^4-q^3-q^2+q)-\frac{q}{12}(q^3-7q+6) \\
&= \frac{1}{12}(3q^4-4q^3+3q^2-2q).
\end{aligned}$$

□

Actually, Theorem 4.4 enables us to do more than just find the cardinality of $G(P_1,P_2)$. It allows us to determine the set $G(P_1,P_2)$. Let $S=\{(\alpha_1,\alpha_2)\in\mathbb{N}_0^2 : \alpha_1+\alpha_2\leq 2g-1\}$. It follows from Lemma 2.1 that $G(P_1,P_2)\subseteq S$. In the following we will use the interval notation $[a,b]$ to mean $\{c\in\mathbb{N}_0 : a\leq c\leq b\}$ and $[a,b]\times[s,t]$ to denote $\{(i,j)\in\mathbb{N}_0^2 : a\leq i\leq b, s\leq j\leq t\}$.

Consider $q-1\in G(P_1)$. By Theorem 4.4, $\beta_{q-1}=q-1$. Since $(0,q),(0,q+1)\in H(P_1,P_2)$, we can apply Lemma 4.1 to get that $(q-1,q),(q-1,q+1)\in H(P_1,P_2)$. Similarly, $(q,q-1),(q+1,q-1)\in H(P_1,P_2)$. Another application of Lemma 4.1 gives $(q,q),(q,q+1),(q+1,q),(q+1,q+1)\in H(P_1,P_2)$. Thus, we get a block $B_{q-1}=[q-1,q+1]\times[q-1,q+1]$ of elements of $H(P_1,P_2)$.

Now consider $q-2\in G(P_1)$. Recall that $\beta_{q-2}=2q-1$. Now since $B_{q-1}\subseteq H(P_1,P_2)$ and $(q-2,2q-1),(0,2q),(0,2q+1),(0,2q+2)\in H(P_1,P_2)$, applying Lemma 4.1 gives that $[q-2,q+1]\times[2q-1,2q+2]\subseteq H(P_1,P_2)$, a 4×4 block B_{q-2} of elements of $H(P_1,P_2)$.

Continuing in this manner, each gap $\alpha=q-i$, $1\leq i\leq q-3$, at P_1 gives an $(i+2)\times(i+2)$ block B_α of elements of $H(P_1,P_2)$.

Now consider $2\in G(P_1)$. From Theorem 4.4, $\beta_2=q^2-2q-1$. Applying Lemma 4.1 as before gives a "triangle" B_2 consisting of $\frac{q(q-1)}{2}$ elements of $H(P_1,P_2)\cap S$. As $\beta_1=2g-1$ and $(1,2g-1)\notin S$, we do not need to consider β_1.

We can continue this process, considering β_α for each gap α at P_1 not in the first column of (1). For $\alpha=(t-j)(q+1)+j\in G(P_1)$, $3\leq j\leq t\leq q-1$, we will get a block $B_\alpha\subseteq S$ of elements of the Weierstrass semigroup of the pair (P_1,P_2).

For $\alpha = (t-2)(q+1)+2 \in G(P_1)$, $2 \leq t \leq q-1$, we will get a "triangle" $B_\alpha \subseteq S$ consisting of $\frac{q(q-1)}{2}$ elements of $H(P_1, P_2)$. Then, by definition of β_α and by Lemma 4.3, all elements of $S \cap \mathbb{N}^2$ which are not in B_α for some $\alpha \in G(P_1)$ are the elements of the Weierstrass gap set $G(P_1, P_2)$ of the pair (P_1, P_2).

Theorem 4.7. *Let P_1 and P_2 be any two distinct Weierstrass points on the Hermitian curve $y^q + y = x^{q+1}$ over $\mathbb{F}_{q^2}$. Then the Weierstrass gap set of the pair (P_1, P_2) is $G(P_1, P_2) = S \setminus [(H(P_1) \times \{0\}) \cup (\{0\} \times H(P_2)) \cup \{B_\alpha : \alpha = (t-j)(q+1)+j, 2 \leq j \leq t \leq q-1\}]$.*

Remark 4.8. Note that the computation of the β_α is independent of the particular choice of Weierstrass points P_1 and P_2 and, thus, so is the set $G(P_1, P_2)$.

Example 4.9. Consider $y^8 + y = x^9$ over $\mathbb{F}_{64}$. Let $P_1 = P_{00}$ and $P_2 = P_\infty$. We use Theorem 4.4 to determine β_α for all gaps α at P_1 and as in (3), write β_α directly beneath α:

(6)

1	2	3	4	5	6	7
55	47	39	31	23	15	7
10	11	12	13	14	15	
46	38	30	22	14	6	
19	20	21	22	23		
37	29	21	13	5		
28	29	30	31			
28	20	12	4			
37	38	39				
19	11	3				
46	47					
10	2					
55						
1						

Next, we apply Lemma 4.1 to find the blocks and "triangles" B_α for α in the first row of (6): $B_7 = [7,9] \times [7,9]$, $B_6 = [6,9] \times [15,18]$, $B_5 = [5,9] \times [23,27]$, $B_4 = [4,9] \times [31,36]$, $B_3 = [3,9] \times [39,45]$, and B_2 is the "triangle" with vertices $(2,47)$, $(8,47)$, and $(2,53)$. Next, we do this for the gaps at P_1 in the second row of (6): $B_{14} = [14,18] \times [14,18]$, $B_{13} = [13,18] \times [22,27]$, $B_{12} = [12,18] \times [30,36]$, and B_{11} is the "triangle" with vertices $(11,38)$, $(17,38)$, and $(11,44)$. Continuing, $B_{21} = [21,27] \times [21,27]$ and B_{20} is the "triangle" with vertices $(20,29)$, $(26,29)$, and $(20,35)$. By symmetry, we determine B_{15}, B_{23}, B_{31}, B_{39}, B_{47}, B_{22}, B_{30}, B_{38}, and B_{29}.

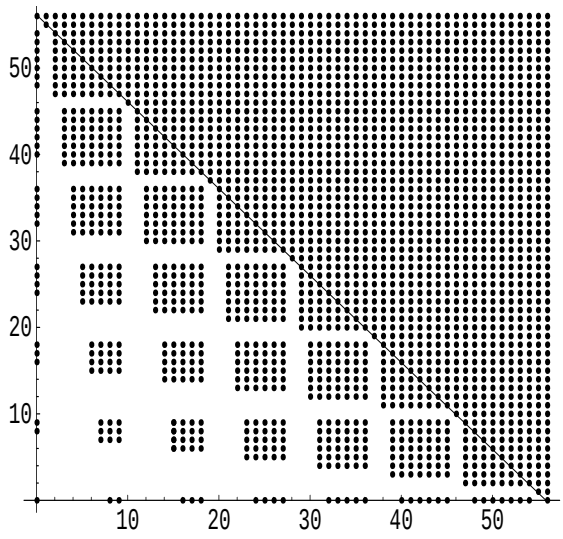

Figure 1

Let T denote the set of all non-negative integers less than $2g+1$. Figure 1 depicts $H(P_1, P_2) \cap T^2$. The line segment in Figure 1 is given by $x + y = 56$. All pairs on this line segment as well as those to the right of or above the line segment are elements of the Weierstrass semigroup $H(P_1, P_2)$ by Lemma 2.1. The Weierstrass gap set $G(P_1, P_2)$ is the complement of the set $H(P_1, P_2) \cap T^2$ in T^2.

5. Results for Codes on Hermitian Curves

Because much is known about Hermitian curves, placing further restrictions on the Weierstrass gap set of a pair may allow one to improve the bound given in Theorem 3.1. Throughout this section, let X denote the Hermitian curve $y^q + y = x^{q+1}$ over $\mathbb{F}_{q^2}$. Recall from the previous section that the Weierstrass gap set of a pair of Weierstrass points on X does not depend on the particular points chosen.

Theorem 5.1. *Consider $C_\Omega(D, G)$ on X with $G = (\alpha_1+\gamma_1-1)P_1+(\alpha_2+\gamma_2-1)P_2$ and $D = Q_1 + \cdots + Q_n$, where P_1, P_2, $Q_1, \ldots, Q_n$ are distinct $\mathbb{F}_{q^2}$-rational points. Suppose $(\alpha_1, \alpha_2) \in G(P_1, P_2)$, $\alpha_1 \geq 1$, and $l(\alpha_1 P_1 + \alpha_2 P_2) = l((\alpha_1 - 1)P_1 + \alpha_2 P_2)$. Also assume $(\gamma_1, \gamma_2-t-1), (\gamma_1+1, \gamma_2-t-1), (\gamma_1+q+1, \gamma_2-t-1), (\gamma_1, \gamma_2) \in G(P_1, P_2)$ for all t, $0 \leq t \leq \min\{\gamma_2 - 1, 2g - 1 - (\alpha_1 + \alpha_2)\}$. If the dimension of this code is positive, then the minimum distance is at least* $\deg G - 2g + 4$.

Proof. Proof Assume $P_1 = P_\infty$. By Theorem 3.1, 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 $(\eta) \geq G - (Q_1 + \cdots + Q_w)$. 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, $A \neq Q_i$ for $1 \leq i \leq w$. Since $l(\alpha_1 P_1 + \alpha_2 P_2) = l((\alpha_1 - 1)P_1 + \alpha_2 P_2)$, there exists a rational function h with divisor

$$(h) = (\alpha_1 - 1)P_1 + (\alpha_2 + t)P_2 - K + E,$$

where E is an effective divisor whose support does not contain P_1 or P_2 and $0 \leq t \leq 2g - 1 - (\alpha_1 + \alpha_2)$. Then

$$G - (Q_1 + \cdots + Q_w) + A = (\eta) \sim K \sim (\alpha_1 - 1)P_1 + (\alpha_2 + t)P_2 + E$$

implies that there exists a rational function f with divisor

$$(f) = -\gamma_1 P_1 - (\gamma_2 - t - 1)P_2 - A + (Q_1 + \cdots + Q_w) + E.$$

First, assume that $t \leq \gamma_2 - 1$. If A is in the support of E, then $(f)_\infty = \gamma_1 P_1 + (\gamma_2 - t - 1)P_2$, contradicting $(\gamma_1, \gamma_2 - t - 1) \in G(P_1, P_2)$. If $A = P_1$, then $(f)_\infty = (\gamma_1 + 1)P_1 + (\gamma_2 - t - 1)P_2$, contradicting $(\gamma_1 + 1, \gamma_2 - t - 1) \in G(P_1, P_2)$. Similarly, $A \neq P_2$, since otherwise $(\gamma_1, \gamma_2 - t) \in H(P_1, P_2)$. Thus, $A = Q_j$ for some j, $w + 1 \leq j \leq n$. Let $\tilde{f}$ denote the rational function on X with divisor $(\tilde{f}) = (q + 1)Q_j - (q + 1)P_1$. Then $(f\tilde{f})_\infty = (\gamma_1 + q + 1)P_1 + (\gamma_2 - t - 1)P_2$, contradicting the fact that $(\gamma_1 + q + 1, \gamma_2 - t - 1) \in G(P_1, P_2)$.

Now suppose $\gamma_2 - 1 < t \leq 2g - 1 - (\alpha_1 + \alpha_2)$. If A is in the support of E or $A = P_2$, then $(f)_\infty = \gamma_1 P_1$. If $A = P_1$, then $(f)_\infty = (\gamma_1 + 1)P_1$. Either case gives a contradiction as γ_1 and $\gamma_1 + 1$ are gaps at P_1. Therefore, $A = Q_j$ for some j, $w + 1 \leq j \leq n$. Then $(f\tilde{f})_\infty = (\gamma_1 + q + 1)P_1$, contradicting the fact that $\gamma_1 + q + 1$ is a gap at P_1. This concludes the proof for the case $P_1 = P_\infty$.

If $P_1 \neq P_\infty$, apply an automorphism φ of X such that $\varphi(P_1) = P_\infty$ [9]. Let ${P_2}' = \varphi(P_2)$. Note that ${P_2}'$ is again a Weierstrass point. Then from the computations in the last section, $G(P_1, P_2) = G(P_\infty, {P_2}')$, and the proof reduces to the case above. □

Proposition 5.2. *Consider a q^2-ary two-point code $C_\Omega(D, G)$ on X satisfying the hypotheses of Theorem 5.1. If* deg $G = 2g + q^2 - aq - b - 3$, $2 \leq a < b \leq q - 1$, *then $C_\Omega(D, G)$ has shorter length and greater minimum distance than that of the one-point code $C_\Omega(D', m'P_\infty)$ on X with the same dimension as $C_\Omega(D, G)$. Furthermore, given any number of the form $r = 2g + q^2 - aq - b - 3$, $2 \leq a < b \leq q - 1$, there is a two-point code $C_\Omega(D, G)$ on X satisfying the hypotheses of Theorem 5.1 such that the degree of the divisor G is r.*

Proof. Proof If deg $G = 2g + q^2 - aq - b - 3$, $2 \leq a < b \leq q - 1$, then $C_\Omega(D, G)$ has dimension $k = q^3 - q^2 + aq + b - g + 1$ and minimum distance at least deg $G - 2g + 4 = q^2 - aq - b + 1$. From [10], the one-point code on X with dimension k is $C_\Omega(D', (2q^2 - (a+1)q - b - 2)P_\infty)$ which is a $[q^3, q^3 - q^2 + aq + b - g + 1, q^2 - aq - b]$ code.

Let $r = 2g + q^2 - aq - b - 3$, $2 \leq a < b \leq q - 1$. Take $(\alpha_1, \alpha_2) = (1, 2g - 2)$ and $(\gamma_1, \gamma_2) = (1, q^2 - aq - b - 1)$ in Theorem 5.1. Theorem 4.4 together with Lemma 2.2 shows that the hypotheses of Theorem 5.1 are satisfied. □

Note that the numbers $2g + q^2 - aq - b - 3$, $2 \leq a < b \leq q - 1$, form a "triangle" with legs of length $q - 3$. This triangle can be formed from the one following Propostion 3.2 by removing the last line.

Remark 5.3. Let $C_\Omega(D, G)$ be a two-point code of dimension k satisfying the hypotheses of Theorem 5.1. Theorem 5.1 allows one to conclude that the two-point

code has shorter length and greater minimum distance than any one-point code of dimension k on X only if the degree of the divisor G is of the form given in Proposition 5.2 or if $\deg G = 2g+q^2-aq-b-3$ with $2 \leq a < q-1$ and $0 \leq b \leq 2$. In the latter case, there is another one-point code with minimum distance d' and dimension greater than k.

Using the fact that there are no places of the Hermitian function field of degree two over $\mathbb{F}_{q^2}$ [3] and placing further restrictions on the gap set $G(P_1, P_2)$ allows one to increase once more the lower bound on the minimum distance of the corresponding two-point code.

Theorem 5.4. *Consider $C_\Omega(D,G)$ on X with $G = (\alpha_1+\gamma_1-1)P_1+(\alpha_2+\gamma_2-1)P_2$ and $D = Q_1+\cdots+Q_n$, where P_1, P_2, $Q_1,\ldots,Q_n$ are distinct $\mathbb{F}_{q^2}$-rational points. Suppose $(\alpha_1,\alpha_2) \in G(P_1,P_2)$, $\alpha_1 \geq 1$, and $l(\alpha_1P_1+\alpha_2P_2) = l((\alpha_1-1)P_1+\alpha_2P_2)$. Also assume that $(\gamma_1,\gamma_2-t-1),(\gamma_1,\gamma_2),(\gamma_1,\gamma_2+1),(\gamma_1+1,\gamma_2-t-1),(\gamma_1+1,\gamma_2),(\gamma_1+2,\gamma_2-t-1),(\gamma_1+q+1,\gamma_2-t-1),(\gamma_1+q+1,\gamma_2),(\gamma_1+q+2,\gamma_2-t-1),(\gamma_1+2q+2,\gamma_2-t-1) \in G(P_1,P_2)$ for all t, $0 \leq t \leq \min\{\gamma_2-1, 2g-1-(\alpha_1+\alpha_2)\}$. If the dimension of $C_\Omega(D,G)$ is positive, then the minimum distance is at least* $\deg G - 2g + 5$.

Proof. Proof By Theorem 5.1, the minimum distance of $C_\Omega(D,G)$ is at least $\deg G - 2g+4$. Put $w = \deg G - 2g+4$. If there is a codeword of weight w, then there exists a differential $\eta \in \Omega(G-D)$ with divisor $(\eta) = G-(Q_1+\cdots+Q_w)+A$ where A is an effective divisor of degree two over $\mathbb{F}_{q^2}$ whose support does not contain Q_i for $1 \leq i \leq w$. Note that there are no places of the Hermitian function field of degree two over $\mathbb{F}_{q^2}$ [3]. Thus $A = 2P_1, 2P_2, P_1+P_2, P_1+Q_i, P_2+Q_i, 2Q_i$, or Q_i+Q_j where $w+1 \leq i,j \leq n$. Using that

$$0 \sim -\gamma_1P_1-(\gamma_2-t-1)P_2-A+(Q_1+\cdots+Q_w)+E,$$

where E is an effective divisor whose support does not contain P_1 or P_2 and $0 \leq t \leq 2g-1-(\alpha_1+\alpha_2)$, and the hypotheses about the gap set of the pair, each possible choice of A can be ruled out. Therefore, the minimum distance is at least $\deg G - 2g + 5$. □

Proposition 5.5. *Consider a q^2-ary two-point code $C_\Omega(D,G)$ on X satisfying the hypotheses of Theorem 5.4. If* $\deg G = 2g+q^2-aq-b-3$, $3 \leq a < b \leq q-1$, *then $C_\Omega(D,G)$ has shorter length and greater minimum distance than that of the one-point code $C_\Omega(D', m'P_\infty)$ on X with the same dimension as $C_\Omega(D,G)$. Furthermore, given any number $r = 2g+q^2-aq-b-3$, $3 \leq a < b \leq q-1$, there is a two-point code $C_\Omega(D,G)$ on X as in Theorem 5.4 such that the degree of the divisor G is r.*

Remark 5.6. Let $C_\Omega(D,G)$ be a two-point code on X of dimension k that satisfies the hypotheses of Theorem 5.4. Theorem 5.4 allows one to conclude that the two-point code has better parameters than any one-point code on X with dimension k only if $\deg G = 2g+q^2-aq-b-3$ where $3 \leq a < b \leq q-1$ or $1 < a \leq q-1$ and $0 \leq b \leq 3$.

6. Examples

Example 6.1. Let X be the hyperelliptic curve of genus 2 over $\mathbb{F}_{16}$ defined by $y^2+y = x^5+1$. Let P_1 be any non-Weierstrass point on X and P_2 be the point at

infinity (on a normalization of X). Then the gap sequence at P_1 is $1, 2$ and the gap sequence at P_2 is $1, 3$. By Lemma 4.3, the Weierstrass gap set of the pair (P_1, P_2) is

$$G(P_1, P_2) = \{(0,1), (0,3), (1,0), (1,1), (1,2), (2,1)\}.$$

Now let $(\alpha_1, \alpha_2) = (1,2)$,$(\gamma_1, \gamma_2) = (1,3)$, and $G = (\alpha_1+\gamma_1-1)P_1+(\alpha_2+\gamma_2-1)P_2 = P_1 + 4P_2$. By Lemma 2.2, $l(P_1 + 2P_2) = l(2P_2)$. Note that $(\gamma_1, \gamma_2 - 1) = (1,2) \in G(P_1, P_2)$. The two-point code $C_\Omega(D, G)$ has dimension 27. Since the Hamming bound tells us that the minimum distance d of this code satisfies $d \leq 4$, Theorem 3.1 allows us to conclude that the minimum distance of $C_\Omega(D, G)$ is exactly 4.

Example 6.2. Let X denote the Hermitian curve $y^4 + y = x^5$ of genus $g = 6$ over $\mathbb{F}_{16}$, $P_1 = P_{00}$, and $P_2 = P_\infty$. Figure 2 depicts $H(P_1, P_2) \cap T^2$, where T denotes the set of non-negative integers less than $2g + 1$. The line segment in Figure 2 is given by $x + y = 12$.

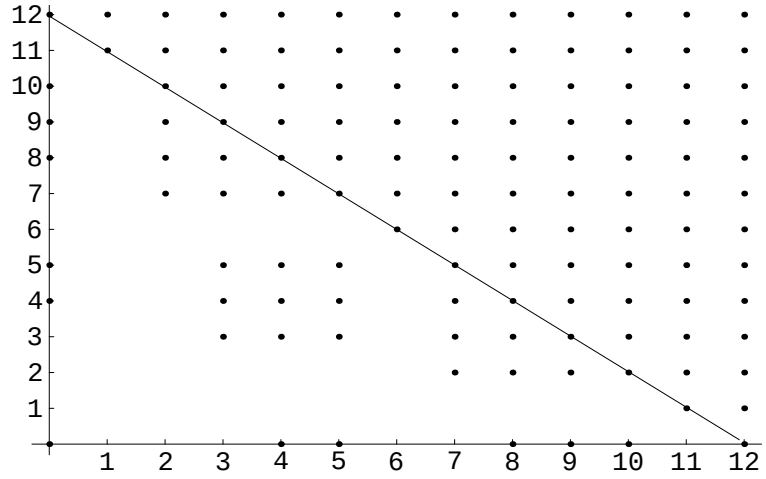

Figure 2

Let $(\alpha_1, \alpha_2) = (6,5)$, $(\gamma_1, \gamma_2) = (3,2)$, and $G = (\alpha_1 + \gamma_1 - 1)P_1 + (\alpha_2 + \gamma_2 - 1)P_2 = 8P_1 + 6P_2$. Note that $(6, \alpha) \in G(P_1, P_2)$ for all α, $0 \leq \alpha \leq 5$, and $(3,1), (4,1), (8,1), (3,2) \in G(P_1, P_2)$. Thus by Lemma 2.2, $l(6P_1 + 5P_2) = l(5P_1 + 5P_2)$. So the hypotheses of Theorem 5.1 hold and the minimum distance d of the two-point code $C_\Omega(D, G)$ is at least 6.

The dimension of $C_\Omega(D, G)$ is $i(G - D) = 54$. So $C_\Omega(D, G)$ is a $[63, 54, \geq 6]$ code. From [10], the only one-point code on X with dimension 54 is $C_\Omega(D', 15P_2)$ which is a $[64, 54, 5]$ code (where D' is the sum of all the $\mathbb{F}_{16}$-rational points other than P_2).

This example also shows that the two-point code $C_\Omega(D, G)$ is not a punctured one-point code as there is no one-point code on X with dimension 54 or greater and minimum distance at least 6 [10].

Example 6.3. Let X denote the Hermitian curve $y^8 + y = x^9$ over $\mathbb{F}_{64}$, $P_1 = P_{00}$, and $P_2 = P_\infty$. Then X has genus $g = 28$. Let $(\alpha_1, \alpha_2) = (1, 54)$, $(\gamma_1, \gamma_2) = (7, 29)$, and $G = (\alpha_1 + \gamma_1 - 1)P_1 + (\alpha_2 + \gamma_2 - 1)P_2 = 7P_1 + 82P_2$. In Section 4 we determined the Weierstrass gap set of the pair (P_1, P_2). Using this, together with

Lemma 2.2, we can see that $l(P_1 + 54P_2) = l(54P_2)$. We can also see that each of the following is an element of the set $G(P_1, P_2)$: $(7, 28)$, $(8, 28)$, $(16, 28)$, $(7, 29)$, $(8, 29)$, $(7, 30)$, $(9, 28)$, $(17, 28)$, $(16, 29)$, and $(25, 28)$. Then, by Theorem 5.4, the minimum distance of the two-point code $C_\Omega(D, G)$ is at least $\deg G - 2g + 5 = 38$. The dimension of $C_\Omega(D, G)$ is $i(G - D) = 449$. So $C_\Omega(D, G)$ is a $[511, 449, \geq 38]$ code while the one-point code on X with dimension 449 is a $[512, 449, 36]$ code according to [10].

7. Acknowledgements

The author wishes to thank A. Garcia for suggesting this problem and R. F. Lax for his help.

References

[1] E. Arbarello, M. Cornalba, P. Griffiths, and J. Harris, *Geometry of Algebraic Curves*, Springer-Verlag, 1985.
[2] 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.
[3] A. Garcia, H. Stichtenoth, and C. P. Xing, *On subfields of the Hermitian function field*, preprint.
[4] V. D. Goppa, *Algebraico-geometric codes*, Math. USSR-Izv. **21** (1983), 75–91.
[5] V. D. Goppa, *Geometry and Codes*, Kluwer, 1988.
[6] M. Homma, *The Weierstrass semigroup of a pair of points on a curve*, Arch. Math. **67** (1996), 337–348.
[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. Stichtenoth, *Algebraic Function Fields and Codes*, Springer-Verlag, 1993.
[9] H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik II*, Arch. Math. **24** (1973), 615–631.
[10] 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.