Contemporary Mathematics

Some computational tools for estimating the parameters of algebraic geometry codes

Gretchen L. Matthews

Abstract. We survey some recent advances in computational tools for determining estimates of the parameters of algebraic geometry codes. We show how the Weierstrass semigroup and its minimal generating set may be used to find the pure gap set as well as floors and ceilings of certain divisors. The code parameter estimates obtained are at least as good as the bounds given by Goppa and in many cases are an improvement.

1. Introduction

Since V. D. Goppa announced the construction of codes from algebraic geometry [**G1**], [**G2**], much work has been done to better understand these codes and their parameters. This interest was piqued by the proof of the existence of a sequence of algebraic geometry codes with parameters exceeding the Gilbert-Varshamov bound [**TVZ**]. In general, it can be very difficult to determine the parameters of an algebraic geometry code. In this paper, we survey some recent advances in computational tools that provide estimates of these parameters that are at least as good as the bounds given by Goppa.

As first suggested by Goppa and later shown in [**GKL**], Weierstrass points can be used to define good codes and Weierstrass gap sets aid in estimating the parameters of such codes. In fact, the Weierstrass gap set of an r-tuple of points on a curve, or its complement the Weierstrass semigroup, has been used to find better bounds on the minimum distances of certain algebraic geometry codes (see [**J**], [**KP**], [**M2**], [**HK**], [**CT**]). Here, we review a method for determining the minimal generating set of a Weierstrass semigroup of a r-tuple of points on a curve. We then show how this minimal generating set may be used to find the set of pure gaps introduced in [**HK**] and floors and ceilings of divisors introduced in [**MMP**] and [**MM**]. These tools have the advantage of being easy to compute using computer algebra packages such as Magma [**BCP**] or Kant [**DFKPRW**]. Finally, we show how this machinery can be used to estimate the parameters of algebraic geometry codes.

Key words and phrases. algebraic geometry code, Riemann-Roch space, Weierstrass gap set, Weierstrass semigroup.

This work was supported in part by NSF grant DMS-0201286.

This paper is organized as follows. Section 2 discusses the computational tools we will be using. Weierstrass semigroups and gap sets are discussed here as well as the floor and the ceiling of a divisor. In Section 3 we demonstrate how these tools may be used to gain information about certain algebraic geometry codes. This section contains examples illustrating applications of the computational tools to codes.

Notation. Let X be a smooth, projective curve of genus $g > 1$ over $\mathbb{F}_q$. Let D_X denote the group of divisors of X over $\mathbb{F}_q$ and $\mathbb{F}_q(X)$ denote the field of rational functions on X defined over $\mathbb{F}_q$. The divisor (resp. pole divisor) of a rational function $f \in \mathbb{F}_q(X)$ is denoted by (f) (resp. $(f)_\infty$). Given a divisor $A \in D_X$, the Riemann-Roch space of A is

$$\mathcal{L}(A) := \{f \in \mathbb{F}_q(X) : (f) \geq -A\} \cup \{0\}.$$

The dimension of the divisor A, denoted $\ell(A)$, is the dimension of the vector space $\mathcal{L}(A)$ over $\mathbb{F}_q$. When comparing elements of $\mathbb{N}_0^r$, we do so with respect to the partial order $\preceq$ defined by $\boldsymbol{\alpha} \preceq \boldsymbol{\alpha'}$ if and only if $\alpha_i \leq \alpha_i'$ for all i, $1 \leq i \leq r$. A code of length n, dimension k, and minimum distance d (resp. at least d) is called an $[n, k, d]$-code (resp. $[n, k, \geq d]$-code).

Let G be a divisor of X and let $D = Q_1 + \cdots + Q_n$ be another divisor of X where $Q_1, \ldots, Q_n$ are distinct $\mathbb{F}_q$-rational points, each not belonging to the support of G. The algebraic geometry codes $C_\mathcal{L}(D, G)$ and $C_\Omega(D, G)$ are constructed as follows:

$$\begin{aligned} &C_\mathcal{L}(D, G) := \{(f(Q_1), f(Q_2), \ldots, f(Q_n)) : f \in \mathcal{L}(G)\} \\ &C_\Omega(D, G) := \{(res_{Q_1}(\eta), res_{Q_2}(\eta), \ldots, res_{Q_n}(\eta)) : \eta \in \Omega(G - D)\}, \end{aligned}$$

where $\Omega(G - D)$ denotes the set of rational differentials η of X over $\mathbb{F}_q$ with divisor $(\eta) \geq G - D$, together with the zero differential. If deg $G < n$, then $C_\mathcal{L}(D, G)$ is an $[n, \ell(G), \geq n - \deg G]$-code. If $2g - 2 <$ deg G, then $C_\Omega(D, G)$ is an $[n, \ell(K + D - G), \geq \deg G - (2g - 2)]$-code. For a general reference on background material, see [**S**] which uses the language of function fields. Here, we find that of algebraic geometry more convenient.

2. Computational tools

In this section, we first review some results on the Weierstrass semigroup of an r-tuple of points on a curve. We then show how the minimal generating set of this semigroup may be used to determine the pure gap set as well as floors and ceilings of certain divisors.

Throughout this section, X will denote a smooth, projective curve of genus $g > 1$ over $\mathbb{F}_q$, and $P_1, \ldots, P_r$ will denote r distinct $\mathbb{F}_q$-rational points on X.

2.1. The Weierstrass gap set. The Weierstrass gap sequence of the point P_1 consists of those nonnegative integers α such that there is no rational function $f \in \mathbb{F}_q(X)$ with pole divisor exactly αP_1. This classically studied object has been generalized to the Weierstrass gap set of a pair of points [**ACGH**] and later to that of an r-tuple of points [**BK**], [**I**]. The Weierstrass semigroup $H(P_1, \ldots, P_r)$ of the r-tuple $(P_1, \ldots, P_r)$ is defined by

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

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

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

The Weierstrass gap set of an r-tuple of points, $r \geq 2$, differs from the Weierstrass gap sequence of a point in that its cardinality depends on the points $P_1, \ldots, P_r$ [**ACGH**], [**K**]. Moreover, facts about numerical semigroups often used to gain information about $H(P_1)$ do not necessarily generalize to results on semigroups of $\mathbb{N}_0^r$, making $H(P_1, \ldots, P_r)$ more difficult to determine. However, as with the Weierstrass gap sequence of a point, one can describe elements of the gap set of an r-tuple of points in terms of dimensions of divisors. This is an immediate generalization of [**K**, Lemma 2.1].

Lemma 2.1. *For $\boldsymbol{\alpha} \in \mathbb{N}^r$, the following are equivalent:*
(i) $\boldsymbol{\alpha} \in H(P_1, \ldots, P_r)$.
(ii) $\ell\left(\sum_{i=1}^r \alpha_i P_i\right) \neq \ell\left(\left(\alpha_j - 1\right) P_j + \sum_{i=1, i \neq j}^r \alpha_i P_i\right)$ for all j, $1 \leq j \leq r$.

While the above result allows one to compute the Weierstrass semigroup (or, equivalently, the Weierstrass gap set), it is not so convenient if one wants to understand the structure of the semigroup or compare two Weierstrass semigroups. At times, it is more suitable to have a smaller generating set to consider. In [**M4**, Theorem 7] it is shown that if $1 \leq r \leq |\mathbb{F}_q|$, then there exists a minimal subset $\Gamma(P_1, \ldots, P_r) \subseteq H(P_1, \ldots, P_r)$ such that

$$H(P_1, \ldots, P_r) = \{\text{lub}\,\{\mathbf{u_1}, \ldots, \mathbf{u_r}\} \in \mathbb{N}_0^r : \mathbf{u_1}, \ldots, \mathbf{u_r} \in \Gamma(P_1, \ldots, P_r)\} \tag{2.1}$$

where $\text{lub}\{\mathbf{u_1}, \ldots, \mathbf{u_r}\} = (\max\{u_{1_1}, \ldots, u_{r_1}\}, \ldots, \max\{u_{1_r}, \ldots, u_{r_r}\}) \in \mathbb{N}_0^r$ is least upper bound of the vectors $\mathbf{u_1}, \ldots, \mathbf{u_r} \in \mathbb{N}_0^r$. The set $\Gamma(P_1, \ldots, P_r)$ is called the minimal generating set of the Weierstrass semigroup $H(P_1, \ldots, P_r)$. Hence, to determine the entire Weierstrass semigroup $H(P_1, \ldots, P_r)$, one only needs to determine the set $\Gamma(P_1, \ldots, P_r)$. This can be done with the help of the next result.

Proposition 2.2. [**M4**, Proposition 9] *For $1 \leq r \leq |\mathbb{F}_q|$ and $\boldsymbol{\alpha} \in \mathbb{N}^r$, the following are equivalent:*

1. *$\boldsymbol{\alpha} \in \Gamma(P_1, \ldots, P_r)$.*
2. *$\ell\left(\sum_{i=1}^r (\alpha_i - 1) P_i\right) = \ell\left(\left(\alpha_j - 1\right) P_j + \sum_{i=1, i \neq j}^r \alpha_i P_i\right)$ for all j, $1 \leq j \leq r$, and $\boldsymbol{\alpha} \in H(P_1, \ldots, P_r)$.*

In the following two subsections, we will see how the Weierstrass semigroup $H(P_1, \ldots, P_r)$ and its minimal generating set $\Gamma(P_1, \ldots, P_r)$ can be used to determine the pure gap set of the r-tuple $(P_1, \ldots, P_r)$ as well as floors and ceilings of divisors supported by the points $P_1, \ldots, P_r$.

2.2. The pure gap set. According to Lemma 2.1, $\boldsymbol{\alpha} \in \mathbb{N}^r$ is an element of the Weierstrass gap set $G(P_1, \ldots, P_r)$ if and only if there exists j, $1 \leq j \leq r$, such that

$$\ell\left(\sum_{i=1}^r \alpha_i P_i\right) = \ell\left(\left(\alpha_j - 1\right) P_j + \sum_{i=1, i \neq j}^r \alpha_i P_i\right). \tag{2.2}$$

In [**HK**] and later in [**CT**], the authors consider those elements of the Weierstrass gap set $G(P_1, \ldots, P_r)$ with "all possible symmetry". More precisely, they consider $\boldsymbol{\alpha} \in \mathbb{N}^r$ such that (2.2) holds for all j, $1 \leq j \leq r$. Such elements of the Weierstrass gap set are called pure gaps. The set of pure gaps of the r-tuple $(P_1, \dots, P_r)$ is denoted by $G_0(P_1, \dots, P_r)$.

The minimal generating set of the Weierstrass semigroup $H(P_1, \dots, P_r)$ may be used to determine the pure gap set $G_0(P_1, \dots, P_r)$. Given i, $1 \le i \le r$, and $\boldsymbol{\alpha} \in G(P_1) \times \cdots \times G(P_r)$, set

$$\Gamma(\boldsymbol{\alpha}, i) := \{\boldsymbol{\gamma} \in \Gamma(P_1, \dots, P_r) : \boldsymbol{\gamma} \preceq \boldsymbol{\alpha}, \gamma_i = \alpha_i\}.$$

Proposition 2.3. *Let $\boldsymbol{\alpha} \in \mathbb{N}^r$. Then $\boldsymbol{\alpha} \in G_0(P_1, \dots, P_r)$ if and only if $\Gamma(\boldsymbol{\alpha}, i) = \emptyset$ for all i, $1 \le i \le r$.*

Proof. First, note that $\boldsymbol{\alpha} \in \mathbb{N}^r$ is a pure gap of the r-tuple $(P_1, \dots, P_r)$ if and only if $\boldsymbol{\alpha'} \in G(P_1, \dots, P_r)$ for all $\boldsymbol{\alpha'} \preceq \boldsymbol{\alpha}$ such that $\alpha'_i = \alpha_i$ for some i, $1 \le i \le r$. Hence, $\boldsymbol{\alpha} \in G_0(P_1, \dots, P_r)$ implies that $\Gamma(\boldsymbol{\alpha}, i) = \emptyset$, for all i, $1 \le i \le r$.

Next, assume that $\Gamma(\boldsymbol{\alpha}, i) = \emptyset$ for all i, $1 \le i \le r$. Suppose $\boldsymbol{\alpha'} \in H(P_1, \dots, P_r)$ satisfies $\boldsymbol{\alpha'} \preceq \boldsymbol{\alpha}$ and $\alpha'_i = \alpha_i$ for some i, $1 \le i \le r$. According to (2.1), there exist $\mathbf{u_1}, \dots, \mathbf{u_r} \in \Gamma(P_1, \dots, P_r)$ such that $\boldsymbol{\alpha'} = \text{lub}\{\mathbf{u_1}, \dots, \mathbf{u_r}\}$. Then $\alpha_i = \alpha'_i = u_{j_i}$ for some j, $1 \le j \le r$. Since $\mathbf{u_j} \preceq \text{lub}\{\mathbf{u_1}, \dots, \mathbf{u_r}\} = \boldsymbol{\alpha'} \preceq \boldsymbol{\alpha}$, $\mathbf{u_j} \in \Gamma(\boldsymbol{\alpha}, i)$ which yields a contradiction. □

Example 2.4. Let X denote a nonsingular model of the projective curve defined by $y^q - y = x^{q_0}(x^q - x)$ over $\mathbb{F}_q$ where $q_0 = 2^n$ and $q = 2^{2n+1}$ for some positive integer n. The genus of X is $q_0(q-1)$ [**HS**]. Note that X has q^2+1 $\mathbb{F}_q$-rational points: q^2 points of the form $P_{ab} := (a : b : 1)$ where $a, b \in \mathbb{F}_q$ and a single point at infinity, P_∞. This curve is known as the Suzuki curve because the automorphism group of X is the Suzuki group of order $q^2(q^2+1)(q-1)$.

Let P_1 and P_2 be distinct $\mathbb{F}_q$-rational points on X. Then $G(P_1) = G(P_2) = \mathbb{N}_0 \setminus \left\langle q, q+q_0, q+\frac{q}{q_0}, q+\frac{q}{q_0}+1 \right\rangle$ [**HS**]. Given $\alpha \in G(P_1)$, write

$$\alpha = \left\lfloor \frac{\alpha}{q+\frac{q}{q_0}+1} \right\rfloor (q + \frac{q}{q_0} + 1) + mq_0 + s$$

where $0 \le s \le q_0 - 1$. Set $j_\alpha := \alpha - \left\lfloor \frac{\alpha}{q+\frac{q}{q_0}+1} \right\rfloor (q + \frac{q}{q_0} + 1) - (k_\alpha - 1)q_0$ where

$$k_\alpha := \begin{cases} m & \text{if } 0 \le s \le \lfloor \frac{m-1}{2} \rfloor + 1 \\ m+1 & \text{if } \lfloor \frac{m-1}{2} \rfloor + 2 \le s \le q_0 - 1. \end{cases}$$

In [**M1**, Theorem 3.3] it is shown that

$$\begin{aligned} \Gamma(P_1, P_2) = \quad & \{(\alpha, 2g-1+q-(q-1)j_\alpha - \alpha) : \alpha \in G(P_1)\} \\ & \cup (H(P_1) \times \{0\}) \cup (\{0\} \times H(P_2)). \end{aligned}$$

According to Proposition 2.3, the pure gap set of the pair (P_1, P_2) is

$$G_0(P_1, P_2) = \{(\alpha, \beta) \in G(P_1) \times G(P_2) : \beta < 2g-1+q-(q-1)j_\alpha - \alpha\}.$$

Example 2.5. Let X be a nonsingular model of the projective curve 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 $m > 2$. If one takes $m = q+1$, the much-studied Hermitian curve is obtained. It can be shown that the genus of X is $\frac{(m-1)(q-1)}{2}$ and that X has exactly $q(m(q-1)+1)+1$ $\mathbb{F}_{q^2}$-rational points [**GV**].

Let $P_1 = P_\infty, P_2 = P_{0b_2}, P_3 = P_{0b_3}, \dots, P_{q+1} = P_{0b_{q+1}}$ be $q+1$ distinct $\mathbb{F}_{q^2}$-rational points on the curve X. Set $c := \frac{q+1}{m}$ and $l := \min\{m, q\}$. Then

$$G(P_i) = \left\{ (t-j)m + j : \begin{array}{c} 1 \le j \le l-1, \\ j \le t \le q-1-j(c-1) \end{array} \right\}$$

for all i, $1 \le i \le q+1$ [**GV**, Theorem 3]. Given $1 \le r \le q+1$, $\mathbf{t} \in \mathbb{N}^r$, and $j \in \mathbb{N}$ such that $1 \le j \le l-1$ and $j \le t_i \le q-1-j(c-1)$ for all $1 \le i \le r$, define

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

According to [**M3**, Theorem 3.7],

$$\Gamma(P_1, \dots, P_r) \cap \mathbb{N}^r = \left\{ \boldsymbol{\gamma}_{\mathbf{t},j} \in \mathbb{N}^r : \sum_{i=1}^r t_i = (m-j)c + r(j-1) \right\}.$$

By Proposition 2.3, $\boldsymbol{\gamma}_{\mathbf{t},j} \in G_0(P_1, \dots, P_r)$ if and only if

$$\left\{ \boldsymbol{\gamma}_{\mathbf{t}',j} \in \mathbb{N}^r : \sum_{i=1}^r t'_i = (m-j)c + r(j-1), t'_i = t_i, t'_k \le t_k \forall k, 1 \le k \le r \right\} = \emptyset$$

for all i, $1 \le i \le r$.

2.3. Floors and ceilings. Given a divisor A of X with $\ell(A) > 0$, it is shown in [**MMP**, Proposition 2.1] that there is a unique divisor $\lfloor A \rfloor$ of X such that

$$\lfloor A \rfloor \in \{A' \in D_X : \mathcal{L}(A') = \mathcal{L}(A)\}$$

and

$$\deg \lfloor A \rfloor = \min\{\deg A' : A' \in D_X, \mathcal{L}(A') = \mathcal{L}(A)\}.$$

The divisor $\lfloor A \rfloor$ is called the floor of A. It is always the case the $\lfloor A \rfloor \le A$. If a spanning set of $\mathcal{L}(A)$ is known, then it can be used to compute the floor of a divisor A [**MMP**, Theorem 2.6]. The Weierstrass semigroup $H(P_1, \dots, P_r)$ provides another way to compute the floors of effective divisors supported by the points $P_1, \dots, P_r$.

Proposition 2.6. *Given $\boldsymbol{\alpha} \in \mathbb{N}^r$, the floor of the divisor $\sum_{i=1}^r \alpha_i P_i$ is given by*

$$\left\lfloor \sum_{i=1}^r \alpha_i P_i \right\rfloor = \sum_{i=1}^r \alpha'_i P_i$$

where $\boldsymbol{\alpha'}$ is maximal in

$$\{\mathbf{a} \in H(P_1, \dots, P_r) : \mathbf{a} \preceq \boldsymbol{\alpha}\}.$$

Proof. Let $A := \sum_{i=1}^r \alpha_i P_i$. Since A is effective, the support of the floor of A is contained in the support of A ([**MMP**, Theorem 2.5]). Thus, $\lfloor A \rfloor = \sum_{i=1}^r \alpha'_i P_i$ for some $\boldsymbol{\alpha'} \in \mathbb{N}_0^r$. By the definition of the floor of a divisor, we have that $\mathcal{L}(\sum_{i=1}^r \alpha'_i P_i - P_j) \ne \mathcal{L}(\sum_{i=1}^r \alpha'_i P_i)$ for all j, $1 \le j \le r$. According to Lemma 2.1, $\boldsymbol{\alpha'} \in H(P_1, \dots, P_r)$. This implies $\boldsymbol{\alpha'} \in \{\mathbf{a} \in H(P_1, \dots, P_r) : \mathbf{a} \preceq \boldsymbol{\alpha}\}$. Suppose that there exists $\mathbf{n} \in \{\mathbf{a} \in H(P_1, \dots, P_r) : \mathbf{a} \preceq \boldsymbol{\alpha}\}$ such that $\boldsymbol{\alpha'} \preceq \mathbf{n}$ and $\boldsymbol{\alpha'} \ne \mathbf{n}$. Then $\alpha'_i < n_i$ for some i, $1 \le i \le r$. Since $\lfloor A \rfloor \le \sum_{i=1}^r n_i P_i \le A$, we have that $\mathcal{L}(\sum_{i=1}^r \alpha'_i P_i) \subseteq \mathcal{L}(\sum_{i=1}^r n_i P_i) \subseteq \mathcal{L}(\sum_{i=1}^r \alpha_i P_i)$. Since $\mathcal{L}(\lfloor A \rfloor) = \mathcal{L}(A)$, it follows that $\mathcal{L}(\lfloor A \rfloor) = \mathcal{L}(\sum_{i=1}^r n_i P_i)$. This is a contradiction according to Lemma 2.1 as $\mathbf{n} \in H(P_1, \dots, P_r)$. □

Let W be a canonical divisor of X and A be a divisor of X with $\ell(W-A)>0$. In [**MM**], we show that there is a unique divisor $\lceil A \rceil$ such that

$$\lceil A \rceil \in \{A' \in D_X : \mathcal{L}(W-A') = \mathcal{L}(W-A)\}$$

and

$$\deg \lceil A \rceil = \max \{\deg A' : A' \in D_X, \mathcal{L}(W-A') = \mathcal{L}(W-A)\}.$$

The divisor $\lceil A \rceil$ is called the ceiling of A. Note that

$$\lceil A \rceil = A + E_{W-A}$$

where $E_{W-A} := W - A - \lfloor W-A \rfloor$. Hence, Proposition 2.6 may also be applied compute the ceiling of a divisor A where $W-A$ is effective.

3. Applications to codes

The notions of pure gaps and floors and ceilings of divisors were motivated by how divisors are used to define algebraic geometry codes. For instance, given effective divisors G and $D := Q_1 + \cdots + Q_n$ where $Q_1, \dots, Q_n$ are distinct $\mathbb{F}_q$-rational points and $\text{supp}G \cap \text{supp}D = \emptyset$, it follows immediately that $C_{\mathcal{L}}(D,G) = C_{\mathcal{L}}(D, \lfloor G \rfloor)$ and so the minimum distance of $C_{\mathcal{L}}(D,G)$ is at least $n - \deg G + \deg(G - \lfloor G \rfloor)$. Similiarly, if $\text{supp}\left(\lceil G-D \rceil + D\right) \cap \text{supp}D = \emptyset$ then $C_\Omega(D,G) = C_\Omega(D, \lceil G-D \rceil + D) = C_\Omega(D, G + E_{W-G+D})$ implies that the minimum distance of $C_\Omega(D,G)$ is at least $\deg(\lceil G-D \rceil + D) - (2g-2) = \deg G - (2g-2) + \deg E_{W-G+D}$. Next, we state a perhaps more interesting application of the floor to give an improved bound on the minimum distance.

Theorem 3.1. [**MM**, Corollary 17] *Let X be a curve over $\mathbb{F}_q$ of genus $g>1$. Let $D := Q_1 + \cdots + Q_n$ where $Q_1, \dots, Q_n$ are distinct $\mathbb{F}_q$-rational points on X, and let $G := H + A$ where H and A are effective divisors of X such that $\lfloor H \rfloor \leq A \leq H$ and the support of H does not contain any of the places $Q_1, \dots, Q_n$. If the code $C_\Omega(D,G)$ is nontrivial, then the minimum distance of $C_\Omega(D,G)$ is at least* $\deg G - (2g-2) + \deg(H-A)$.

Corollary 3.2. [**CT**, Theorem 3.4] *Let X be a curve over $\mathbb{F}_q$ of genus $g>1$ and let $D := Q_1 + \cdots + Q_n$ where $Q_1, \dots, Q_n, P_1, \dots, P_r$ are distinct $\mathbb{F}_q$-rational points on X. Suppose $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are pure gaps of the r-tuple of points $(P_1, \dots, P_r)$ such that $\boldsymbol{\beta} - \boldsymbol{\alpha} \succeq \mathbf{0}$ and $\boldsymbol{\delta} \in G_0(P_1, \dots, P_r)$ for all $\boldsymbol{\delta}, \boldsymbol{\alpha} \preceq \boldsymbol{\delta} \preceq \boldsymbol{\beta}$. Set $G = \sum_{i=1}^r (\alpha_i + \beta_i - 1)P_i$. If the code $C_\Omega(D,G)$ is nontrivial, then it has minimum distance at least* $\deg G - (2g-2) + (\sum_{i=1}^r \beta_i - \alpha_i) + r$.

Proof. Let $H = \sum_{i=1}^r \beta_i P_i$ and $A = \sum_{i=1}^r (\alpha_i - 1)P_i$. Since $\boldsymbol{\delta} \in G_0(P_1, \dots, P_m)$ for all $\boldsymbol{\alpha} \preceq \boldsymbol{\delta} \preceq \boldsymbol{\beta}$, $\mathcal{L}(A) = \mathcal{L}(H)$. Hence, $\lfloor H \rfloor \leq A \leq H$. Then Theorem 3.1 applies to give

$$d \geq \deg G - (2g-2) + \deg(H-A) = \deg G - (2g-2) + \sum_{i=1}^r (\beta_i - \alpha_i + 1).$$

□

Example 3.3. Let X denote a nonsingular model of 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. According to Proposition 2.6 and the minimal generating set given in Example 2.5, the floor of $9P_\infty+P_{00}+P_{01}$ is

$$\lfloor 9P_\infty + P_{00} + P_{01}\rfloor = 9P_\infty.$$

Let D be the sum of all 174 $\mathbb{F}_{64}$-rational points other than P_∞, P_{00}, and P_{01}. Then Theorem 3.1 applies showing that $C_\Omega(D, 18P_\infty + P_{00} + P_{01})$ is a $[174, 160, \geq 10]$-code. This code can be compared with the one-point Hermitian code over $\mathbb{F}_{64}$ with a similar information rate. According to [**YK**], $C_\Omega(D + P_{00} + P_{01}, 69P_\infty)$ is a $[512, 470, 16]$-code which has information rate $\frac{470}{512} \approx 0.91797$ and relative distance $\frac{16}{512} = 0.03125$. The code $C_\Omega(D, 18P_\infty + P_{00} + P_{01})$ has information rate $\frac{160}{174} \approx 0.91954$ and relative distance at least $\frac{10}{174} \approx 0.05747$, both greater than that of the comparable one-point Hermitian code over $\mathbb{F}_{64}$.

Example 3.4. Consider the Suzuki curve X over $\mathbb{F}_8$ which is defined by

$$y^8 - y = x^2(x^8 - x).$$

Note that the genus of X is 14. Recall that the Weierstrass semigroup of the point P_∞ is $H(P_\infty) = \langle 8, 10, 12, 13\rangle$. According to Proposition 2.6, the floor of $15P_\infty$ is $\lfloor 15P_\infty\rfloor = 13P_\infty$. Let D be the sum of all 64 $\mathbb{F}_8$-rational points on X other than P_∞. Then $C_\mathcal{L}(D, 15P_\infty) = C_\mathcal{L}(D, 13P_\infty)$ and so is a $[64, 5, \geq 64 - 13 = 51]$-code over $\mathbb{F}_8$. In [**CD**], it is shown that $C_\mathcal{L}(D, 15P_\infty)$ is a $[64, 5, 51]$-code. Moreover, this is a best known code of length 64 and dimension 5 over $\mathbb{F}_8$ [**B**].

Now let D be the sum of all 63 $\mathbb{F}_8$-rational points on X other than P_∞ and P_{00}. Take $H = 23P_\infty + P_{00}$. Then Proposition 2.6 and Example 2.4 imply that

$$\lfloor 23P_\infty + P_{00}\rfloor = 23P_\infty.$$

As a result, Theorem 3.1 applies to give that $C_\Omega(D, 46P_\infty + P_{00})$ is a $[63, 29, \geq 22]$-code. This is a best known code of length 63 and dimension 29 over $\mathbb{F}_8$ [**B**].

References

[ACGH] E. Arbarello, M. Cornalba, P. Griffiths, and J. Harris, Geometry of Algebraic Curves, Springer-Verlag, 1985.

[BK] E. Ballico and S. J. Kim, Weierstrass multiple loci of n-pointed algebraic curves, J. Algebra **199** (1998), 455–471.

[BCP] W. Bosma, J. Cannon, C. Playoust, The MAGMA algebra system, I: The user language, J. Symb. Comp. **24** (1997), 235–265.

[B] A. E. Brouwer, Linear code bounds,
`http://www.win.tue.nl/ aeb/voorlincod.html`, April 2004.

[CT] C. Carvalho and F. Torres, On Goppa codes and Weierstrass gaps at several points, preprint.

[CD] C. Y. Chen and I. Duursma, Geometric Reed-Solomon codes of length 64 and 65 over $\mathbb{F}_8$, IEEE Trans. on Inform. Theory **49** (2003), no. 5, 1351–1353.

[DFKPRW] M. Daberkow, C. Fieker, J. Klüners, M. Pohst, K. Roegner and K. Wildanger, *KANT V4*, in J. Symbolic Comp. **24** (1997), 267-283.

[GKL] 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.

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

[G1] V. D. Goppa, Algebraico-geometric codes, Math. USSR-Izv. **21** (1983), 75–91.

[G2] V. D. Goppa, Geometry and Codes, Kluwer, 1988.

[HS] J. P. Hansen and H. Stichtenoth, Groupcodes on certain algebraic curves with many rational points, Appl. Algebra Engrg. Comm. Comput. **1** (1990), 67-77.

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

[I] N. Ishii, A certain graph obtained from a set of several points on a Riemann surface, Tsukuba J. Math. **23** (1999), no. 1, 55–89.

[J] H. Janwa, On the parameters of algebraic geometry codes, Applied Algebra, Algebraic Algorithms, and Error-correcting Codes (New Orleans, LA, 1991), Lecture Notes in Computer Science **539**, Springer, Berlin 1991, 19–28.

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

[KP] C. Kirfel and R. Pellikaan, The minimum distance of codes in an array coming from telescopic semigroups, IEEE Trans. Inform. Theory **41** no. 5 part 1 (1995), 1720–1732.

[MM] H. Maharaj and G. L. Matthews, On the floor and the ceiling of a divisor, in review.

[MMP] 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, J. Pure Appl. Algebra, to appear.

[M1] G. L. Matthews, Codes from the Suzuki function field, IEEE Trans. Inform. Theory, to appear.

[M2] G. L. Matthews, Weierstrass pairs and minimum distance of Goppa codes, Des. Codes and Cryptog. **22** (2001), 107–121.

[M3] G. L. Matthews, Weierstrass semigroups and codes from a quotient of the Hermitian curve, in review.

[M4] G. L. Matthews, The Weierstrass semigroup of an m-tuple of collinear points on a Hermitian curve, Lecture Notes in Comput. Sci. **2948** (2004), 12–24.

[S] H. Stichtenoth, Algebraic Function Fields and Codes, Springer, Berlin, 1993.

[TVZ] M. A. Tsfasman, S. G. Vlǎdut, and T. Zink, Modular curves, Shimura curves, and Goppa codes better than the Varshamov-Gilbert bound, Math. Nachrichtentech. **109** (1982), 21–28.

[YK] K. Yang and P. V. Kumar, On the true minimum distance of Hermitian codes, Coding Theory and Algebraic Geometry, Lecture Notes in Math. (1992), 99–107.

Department of Mathematical Sciences, Clemson University, Clemson, South Carolina 29634-0975

E-mail address: gmatthe@clemson.edu