ONE-POINT CODES USING PLACES OF HIGHER DEGREE

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

Abstract. In (IEEE Trans. Inform. Theory **48** no. 2 (2002), 535–537), Xing and Chen show that there exist algebraic geometry codes from the Hermitian function field over $\mathbb{F}_{q^2}$ constructed using $\mathbb{F}_{q^2}$-rational divisors which are improvements over the much-studied one-point Hermitian codes. In this paper, we construct such codes by using a place P of degree $r > 1$. This motivates a study of gap numbers and pole numbers at places of higher degree. In fact, the code parameters are estimated using the Weierstrass gap set of the place P and relating it to the gap set of the r-tuple of places of degree one lying over P in a constant field extension of degree r.

1. Introduction

An algebraic geometry (AG) code over $\mathbb{F}_q$ is defined using two divisors G and D of a function field $F/\mathbb{F}_q$. Typically, the divisor G is taken to be a multiple of a single place of F of degree one and $D := Q_1 + \cdots + Q_n$ is supported by n distinct places of degree one different from the place in the support of G. Such a code is called a one-point code. It has been shown that better AG codes may be obtained by allowing the divisor G to be more general (see [6], [4], [9], [2]). In particular, Xing and Chen have shown that there exist $\mathbb{F}_{q^2}$-rational divisors G of the Hermitian function field over $\mathbb{F}_{q^2}$ such that $C_{\mathcal{L}}(D, G)$ has better parameters than the comparable one-point Hermitian code [9]. In this paper, we consider the special case where $G = \alpha P$ and P is a place of F of degree greater than one. Such codes may be thought of as one-point codes defined using places of higher degree. This construction differs from that of generalized AG codes, or XNL codes, proposed by Niederreiter, Xing, and Lam [10] in which the divisor D, rather than G, may be supported by places of higher degree.

To study one-point codes constructed using places of higher degree, we first consider the Weierstrass gap set of a place of higher degree. In doing so, it is helpful to examine the Weierstrass gap set of an r-tuple of places of degree one in a constant field extension. This allows one to use theory that has been developed in applications of Weierstrass gap sets of r-tuples of places to codes [4], [2]. As a result, we obtain explicit constructions for one-point codes using places of higher degree that have better parameters than the comparable classical one-point code from the same function field. Moreover, we define specific codes with parameters comparable to (and, at times, better than) those found in [9].

This project was supported by NSF DMS-0201286.

This paper is organized as follows. First, we review the notation used throughout the paper. In Section 2, the Weierstrass gap set of a place of higher degree is discussed. Constant field extensions are utilized to better understand this set. In Section 3, applications to codes are considered. Finally, examples are given to illustrate these methods.

Notation. Unless stated otherwise, we will use notation as in [8].

Let $F/\mathbb{F}_q$ be an algebraic function field of genus $g > 1$. The divisor (resp. pole divisor) of a function $f \in F$ will be denoted by $(f)^F$ (resp. $(f)_\infty^F$), or simply (f) (resp. $(f)_\infty$) if the context is clear. Let Ω denote the set of rational differentials of $F/\mathbb{F}_q$. The divisor of a differential $\eta \in \Omega$ will be denoted by (η) and the residue of η at a place P will be denoted by $res_P(\eta)$. Given a divisor A of F, let $\mathcal{L}(A) := \{f \in F \setminus \{0\} : (f) \geq -A\} \cup \{0\}$ and $\Omega(A) := \{\eta \in \Omega \setminus \{0\} : (\eta) \geq A\} \cup \{0\}$. Let $\ell(A)$ denote the dimension of the vector space $\mathcal{L}(A)$ over $\mathbb{F}_q$. The Riemann-Roch Theorem states that

$$\ell(A) = \deg A + 1 - g + \ell(W - A)$$

where W is any canonical divisor of F. Moreover, if the degree of A is at least $2g-1$, then $\ell(W - A) = 0$ and so $\ell(A) = \deg A + 1 - g$. As usual, 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 sometimes write $d(C)$ to mean the minimum distance of the code C. The set of positive integers is denoted by $\mathbb{N}$ and the set of nonnegative integers is denoted by $\mathbb{N}_0$.

Let G be a divisor of $F/\mathbb{F}_q$ and let $D = Q_1 + \cdots + Q_n$ be another divisor of $F/\mathbb{F}_q$ where $Q_1, \ldots, Q_n$ are distinct places of F of degree one, each not contained in the support of G. The algebraic geometry (AG) code $C_\Omega(D, G)$ is defined by

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

and is an $[n, \ell(G - D) - \ell(G) + \deg D, \geq \deg G - (2g - 2)]$-code.

2. Gaps at places of higher degree

Let $F/\mathbb{F}_q$ be an algebraic function field of genus $g > 1$, and let P be a place of F of degree r. Define the Weierstrass semigroup of the place P by

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

and the Weierstrass gap set of the place P by

$$G(P) := \mathbb{N}_0 \setminus H(P).$$

Elements of the set $G(P)$ are often referred to as gaps at the place P. One can easily check that the set $H(P)$ is an additive submonoid of $\mathbb{N}_0$. It is also easy to see that given $\alpha \in \mathbb{N}_0$, $\alpha \in H(P)$ if and only if $\ell(\alpha P) \neq \ell((\alpha - 1)P)$.

Recall that the Weierstrass Gap Theorem states that given a place P of F of degree one, there are exactly g gaps at P and each element of the Weierstrass gap set lies in the interval $[1, 2g-1]$. In the next two propositions, we consider analogous results for places of degree possibly greater than one.

Proposition 2.1. *Let P be a place of $F/\mathbb{F}_q$ of degree r. If $\alpha > \left\lceil \frac{2g-1}{r} \right\rceil$, then $\alpha \in H(P)$. Moreover, $G(P) \subseteq [1, \left\lfloor \frac{2g-1}{r} \right\rfloor]$.*

Proof. Set $s = r\left\lceil \frac{2g-1}{r}\right\rceil - (2g-1)$ and suppose $\alpha > \left\lceil \frac{2g-1}{r}\right\rceil = \frac{2g-1+s}{r}$. Then $\alpha r > (\alpha-1)\, r \geq 2g-1+s$, which implies $\ell(\alpha P) > \ell((\alpha-1)P)$ by the Riemann-Roch Theorem. Hence, $\alpha \in H(P)$.

Clearly, $0 \in H(P)$ as $(a)_\infty = 0P$ for $a \in \mathbb{F}_q$. Thus, $G(P) \subseteq [1, \left\lceil \frac{2g-1}{r}\right\rceil]$. It remains to show that if $r \nmid 2g-1$ then $\left\lceil \frac{2g-1}{r}\right\rceil \in H(P)$. Suppose $\alpha = \left\lceil \frac{2g-1}{r}\right\rceil = \frac{2g-1+s}{r}$ where $r > 1$. Note that $0 < s \leq r-1$. Then $\alpha r > 2g-1$ which implies $\ell(\alpha P) = \alpha r + 1 - g$. By Clifford's Theorem, $\ell(W-(\alpha-1)P) \leq 1 + \frac{1}{2}\,(r-s-1) < 1 + \frac{1}{2}\,(r-1)$ for any canonical divisor W. It follows that

$$\begin{aligned} \ell(\alpha P) - \ell((\alpha-1)P) &= \alpha r + 1 - g - (\alpha-1)r - 1 + g - \ell(W-(\alpha-1)P) \\ &\geq r - \ell(W-(\alpha-1)P) \\ &> \tfrac{1}{2}(r-1) > 0 \end{aligned}$$

as $r > 1$. Therefore, $\alpha \in H(P)$ and so $G(P) \subseteq [1, \left\lceil \frac{2g-1}{r}\right\rceil - 1] = [1, \left\lfloor \frac{2g-1}{r}\right\rfloor]$. □

Proposition 2.2. *Let P be a place of $F/\mathbb{F}_q$ of degree r. Then*

$$g = \left(\sum_{i=0}^{\left\lceil \frac{2g-1}{r}\right\rceil} \ell(iP) - \ell((i-1)P) \right) - s$$

where $s = r\left\lceil \frac{2g-1}{r}\right\rceil - (2g-1)$.

Proof. By the Riemann-Roch Theorem, $\ell\left(\left\lceil \frac{2g-1}{r}\right\rceil P\right) = g+s$. Then

$$0 = \ell(-1P) \leq \ell(0P) \leq \ell(P) \leq \ell(2P) \leq \cdots \leq \ell\left(\left\lceil \frac{2g-1}{r}\right\rceil P\right) = g+s.$$

Hence, $g+s = \ell\left(\left\lceil \frac{2g-1}{r}\right\rceil P\right) - \ell(-1P) = \sum_{i=0}^{\left\lceil \frac{2g-1}{r}\right\rceil} \ell(iP) - \ell((i-1)P)$. □

Notice that if one takes $r = 1$ in the above proposition, then this shows that the number of gaps at P is the genus of F, as $s = 0$ and $0 \leq \ell(iP) - \ell((i-1)P) \leq 1$. However, if P is a place of degree $r > 1$, then it is not necessarily the case that $\ell(iP) - \ell((i-1)P) \in \{0, r\}$ for each $i \in \mathbb{N}$. Lewittes [5] has shown that $g = \sum_{i=1}^{\infty} r - (\ell(iP) - \ell((i-1)P))$. From the proof of Proposition 2.1, we see that $r - (\ell(iP) - \ell((i-1)P)) = 0$ for all $i > \left\lceil \frac{2g-1}{r}\right\rceil$. Thus, Lewittes' result can be improved to give

$$g = \sum_{i=1}^{\left\lceil \frac{2g-1}{r}\right\rceil} r - (\ell(iP) - \ell((i-1)P)).$$

Next, we show how the Weierstrass semigroup of an r-tuple of places of degree one in a constant field extension may be used to study that of a place of degree r. Let $F' := \mathbb{F}_{q^r}F/\mathbb{F}_{q^r}$ be a constant field extension of $F/\mathbb{F}_q$ of degree r. Then the place P splits completely in F'. Hence, there are r distinct places $P_1, \ldots, P_r \in \mathbb{P}_{F'}$ of degree one lying over the place P:

$$\begin{tikzcd} F' := \mathbb{F}_{q^r}F \arrow[d, dash] & P_1, \ldots, P_r \arrow[d, dash] \\ F & P \end{tikzcd}$$

By definition, the conorm of αP is $Con_{F'/F}(\alpha P) = \alpha P_1 + \cdots + \alpha P_r$ for all $\alpha \in \mathbb{N}$. According to [8, Theorem III.6.3],

$$\ell(Con_{F'/F}(\alpha P)) = \ell(\alpha P)$$

for all $\alpha \in \mathbb{N}$. Hence,

$$(1) \quad \ell(\alpha P) - \ell((\alpha-1)P) = \ell(\alpha P_1 + \cdots + \alpha P_r) - \ell((\alpha-1)P_1 + \cdots + (\alpha-1)P_r).$$

It is very natural to relate the Weierstrass semigroup $H(P)$ to that of the r-tuple $(P_1, \dots, P_r)$. Given m distinct places $Q_1, \dots, Q_m$ of degree one of F, the Weierstrass semigroup $H(Q_1, \dots, Q_m)$ of the m-tuple $(Q_1, \dots, Q_m)$ is defined by

$$H(Q_1, \dots, Q_m) = \left\{ \boldsymbol{\alpha} \in \mathbb{N}_0^m : \exists f \in F \text{ with } (f)_\infty = \sum_{i=1}^{m} \alpha_i Q_i \right\},$$

and the Weierstrass gap set $G(Q_1, \dots, Q_m)$ of the m-tuple $(Q_1, \dots, Q_m)$ is defined by

$$G(Q_1, \dots, Q_m) = \mathbb{N}_0^m \setminus H(Q_1, \dots Q_m).$$

Proposition 2.3. *Let P be a place of degree r of a function field $F/\mathbb{F}_q$ and $P_1, \dots, P_r$ be the extensions of P in the constant field extension F' of F of degree r. Given $\alpha \in \mathbb{N}$, $\alpha \in H(P)$ if and only if $(\alpha, \dots, \alpha) \in H(P_1, \dots, P_r)$.*

Proof. Suppose $\alpha \in H(P)$. Then there is a function $f \in F$ with divisor

$$(f)^F = A - \alpha P$$

where $P \notin \operatorname{supp} A$. By [8, Proposition III.1.9],

$$(f)^{F'} = Con_{F'/F}(A) - \alpha P_1 - \cdots - \alpha P_r$$

which implies $(\alpha, \dots, \alpha) \in H(P_1, \dots, P_r)$.

Suppose $(\alpha, \dots, \alpha) \in H(P_1, \dots, P_r)$. Then

$$\ell(\alpha P_1 + \cdots + \alpha P_r) = \ell(\alpha P_1 + \cdots + (\alpha-1)P_i + \cdots + \alpha P_r) + 1$$

for all $1 \le i \le r$. From (1), it follows that $\ell(\alpha P) \neq \ell((\alpha-1)P)$. Consequently, $\alpha \in H(P)$. □

From the above result, $\alpha \in G(P)$ if and only if $(\alpha, \dots, \alpha) \in G(P_1, \dots, P_r)$. It turns out that much more is true. Notice that $\boldsymbol{\alpha} \in \mathbb{N}^r$ is an element of the Weierstrass gap set $G(P_1, \dots, P_r)$ if and only if there exists j, $1 \le j \le r$, such that

$$(2) \qquad \ell\left(\sum_{i=1}^{r} \alpha_i P_i\right) = \ell\left((\alpha_j - 1)P_j + \sum_{i=1, i\neq j}^{r} \alpha_i P_i\right).$$

In [4] and later in [2], the authors consider those elements of the Weierstrass gap set $G(P_1, \dots, P_r)$ with "all possible symmetry". More precisely, they consider $\boldsymbol{\alpha} \in \mathbb{N}^r$ satisfying (2) for all j, $1 \le j \le r$. 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 $G_0(P_1, \dots, P_r)$. In [2, Lemma 2.5], it is shown that $\boldsymbol{\alpha} \in G_0(P_1, \dots, P_r)$ if and only if $\ell\left(\sum_{i=1}^{r} \alpha_i P_i\right) = \ell\left(\sum_{i=1}^{r} (\alpha_i - 1) P_i\right)$.

Proposition 2.4. *Let P be a place of degree r of a function field $F/\mathbb{F}_q$ and $P_1, \dots, P_r$ be the extensions of P in the constant field extension of F of degree r. Suppose that $\alpha, \dots, \alpha + t \in G(P)$. Then $[\alpha, \alpha+t]^r \subseteq G_0(P_1, \dots, P_r)$.*

Proof. Suppose there exists $\mathbf{v} \in [\alpha, \alpha+t]^r$ such that $\mathbf{v} \notin G_0(P_1, \dots, P_r)$. Then

$$\ell\left(\sum_{i=1}^{r} v_i P_i\right) \neq \ell\left((v_j - 1)P_j + \sum_{i=1, i\neq j}^{r} v_i P_i\right)$$

for some j, $1 \leq j \leq r$. Then

$$\begin{array}{rcl} \ell((\alpha-1)P) & = & \ell\left(\sum_{i=1}^{r}(\alpha-1)P_i\right) \\ & \leq & \ell\left((v_j-1)P_j + \sum_{i=1, i\neq j}^{r} v_i P_i\right) \\ & < & \ell\left(\sum_{i=1}^{r} v_i P_i\right) \\ & \leq & \ell\left(\sum_{i=1}^{r}(\alpha+t)P_i\right) \\ & = & \ell((\alpha+t)P) \end{array}$$

which is a contradiction as $\alpha, \ldots, \alpha+t \in G(P)$ implies that

$$\ell((\alpha-1)P) = \ell(\alpha P) = \cdots = \ell((\alpha+t)P).$$

□

Example 2.5. Consider the function field $F := \mathbb{F}_q(x,y)/\mathbb{F}_q$ where $y^q + y = x^{q+1}$. Let P be a place of F of degree two. We claim that the Weierstrass semigroup of the place P is

$$H(P) = \langle q-1, q, q+1 \rangle$$

where $\langle a_1, \ldots, a_t \rangle := \left\{ \sum_{i=1}^{t} c_i a_i : c_i \in \mathbb{N}_0 \right\}$.

There are exactly two places of degree one, P_1 and P_2, in the constant field extension $F' := \mathbb{F}_{q^2}F$ lying over P. Note that $F'/\mathbb{F}_{q^2} = \mathbb{F}_{q^2}(x,y)/\mathbb{F}_{q^2}$ is the Hermitian function field over $\mathbb{F}_{q^2}$. It is well known that the Weierstrass semigroup of any place of $F'/\mathbb{F}_{q^2}$ of degree one is $\langle q, q+1 \rangle$. In [6, Theorem 3.7], the Weierstrass semigroup of any pair of places of $F'/\mathbb{F}_{q^2}$ of degree one is determined. Next, we use these two facts to find $H(P)$. Clearly, according to Proposition 2.3,

$$\begin{array}{rcl} H(P) & = & \{\alpha \in \mathbb{N}_0 : (\alpha, \alpha) \in H(P_1, P_2)\} \\ & = & \{\alpha \in H(P_1) : (\alpha,\alpha) \in H(P_1,P_2)\} \cup \{\alpha \in G(P_1) : (\alpha,\alpha) \in H(P_1,P_2)\} \\ & = & \langle q, q+1 \rangle \cup \{\alpha \in G(P_1) : (\alpha,\alpha) \in H(P_1,P_2)\}. \end{array}$$

By [6, Theorem 3.7], $\alpha \in G(P_1)$ and $(\alpha,\alpha) \in H(P_1,P_2)$ implies $\alpha \in \langle q-1 \rangle$. Thus,

$$H(P) = \langle q, q+1 \rangle \cup \langle q-1 \rangle \subseteq \langle q-1, q, q+1 \rangle.$$

Now suppose that $\alpha = a(q-1) + bq + c(q+1)$ with $a, b, c \in \mathbb{N}_0$. By [6, Theorem 3.4] and Proposition 2.3, $a(q-1) \in H(P)$. Since $H(P_1) = H(P_2) = \langle q, q+1 \rangle$, Proposition 2.3 implies that $bq + c(q+1) \in H(P)$. It follows that $\alpha \in H(P)$ as $H(P)$ is closed under addition. Therefore, $H(P) = \langle q-1, q, q+1 \rangle$.

3. One point codes using places of higher degree

In this section, we consider AG codes $C_\Omega(D, \alpha P)$ over $\mathbb{F}_q$ where P is a place of $F/\mathbb{F}_q$ of degree greater than one. The next lemma illustrates how a code of this form relates to the code $C_\Omega(Con_{F'/F}(D), Con_{F'/F}(\alpha P))$.

Lemma 3.1. *Let G and $D := Q_1 + \cdots + Q_n$ be divisors of $F/\mathbb{F}_q$ where $Q_1, \ldots, Q_n$ are distinct places of degree one of F, none of which are contained in the support of G. Set $r := \max\{\deg P : P \in \text{supp } G\}$. Let $F' := F\mathbb{F}_{q^r}/\mathbb{F}_{q^r}$ be a constant field extension of $F/\mathbb{F}_q$ of degree r. Then the two codes $C_\Omega(D,G)$ and $C_\Omega(Con_{F'/F}(D), Con_{F'/F}(G))$ have the same length. The dimension of $C_\Omega(D,G)$ (over $\mathbb{F}_q$) is equal to that of $C_\Omega(Con_{F'/F}(D), Con_{F'/F}(G))$ (over $\mathbb{F}_{q^r}$). The minimum distance of $C_\Omega(D,G)$ is at least that of $C_\Omega(Con_{F'/F}(D), Con_{F'/F}(G))$.*

Proof. Clearly, $Con_{F'/F}(D) = Q_1 + \cdots + Q_n$ as each Q_i has degree one, and the dimension of $C_\Omega(D,G)$ is $\ell(G-D) - \ell(G) + \deg D = \ell(Con_{F'/F}(G) - Con_{F'/F}(D)) - \ell(Con_{F'/F}(G)) + \deg Con_{F'/F}(D)$, the dimension of $C_\Omega(Con_{F'/F}(D), Con_{F'/F}(G))$. Let d denote the minimum distance of $C_\Omega(D,G)$. Suppose that $\eta \in \Omega(G-D)$ and that the weight of $(res_{Q_1}(\eta), \ldots, res_{Q_n}(\eta))$ is equal to d. Without loss of generality, we may assume that $(\eta) \geq G - (Q_1 + \cdots + Q_d)$. Then $Con_{F'/F}((\eta))$ is a canonical divisor of $F'/\mathbb{F}_{q^r}$ and $Con_{F'/F}((\eta)) \geq Con_{F'/F}(G) - Con_{F'/F}(Q_1 + \cdots + Q_d)$ which implies that $C_\Omega(Con_{F'/F}(D), Con_{F'/F}(G))$ has a codeword of weight d. □

The pure gap set of a pair of places of degree one is used to define codes with minimum distance greater than the usual lower bound in [4]. This is generalized to r-tuples of places of degree one in [2]. These results together with those in Section 2 will be applied to obtain better bounds on the minimum distance of codes defined using elements of the gap set of a place of higher degree. For convenience, we include here the two results from [2] that we will use.

Lemma 3.2. [2, Theorem 3.3] *Let $Q_1, \ldots, Q_n, P_1, \ldots, P_m$ be distinct places of $F/\mathbb{F}_q$ such that* $\deg Q_i = 1$ *for each i, $1 \leq i \leq n$. Set $D' := Q_1 + \cdots + Q_n$. Suppose $G' := \sum_{i=1}^m (a_i + b_i - 1)P_i$ where $\mathbf{a}, \mathbf{b} \in G_0(P_1, \ldots, P_m)$. If the code $C_\Omega(D', G')$ is nontrivial, then it has minimum distance at least* $\deg G' - (2g-2) + m$.

Lemma 3.3. [2, Theorem 3.4] *Let $Q_1, \ldots, Q_n, P_1, \ldots, P_m$ be distinct places of $F/\mathbb{F}_q$ such that* $\deg Q_i = 1$ *for each i, $1 \leq i \leq n$. Set $D' := Q_1 + \cdots + Q_n$. Suppose $G' := \sum_{i=1}^m (a_i + b_i - 1)P_i$ where $\mathbf{v} \in G_0(P_1, \ldots, P_m)$ for all $\mathbf{v} \in \mathbb{N}_0^m$ such that $\mathbf{a} \preceq \mathbf{v} \preceq \mathbf{b}$. If the code $C_\Omega(D', G')$ is nontrivial, then it has minimum distance at least* $\deg G' - (2g-2) + \sum_{i=1}^m (b_i - a_i + 1)$.

We can modify Lemma 3.2 to get an analog of [3, Theorem 1] for codes defined using places of higher degree.

Theorem 3.4. *Let P be a place of degree r and $Q_1, \ldots, Q_n$ be distinct places of $F/\mathbb{F}_q$ of degree one such that $Q_i \neq P$ for each i, $1 \leq i \leq n$. Set $D := Q_1 + \cdots + Q_n$. Suppose $G := (\alpha + \beta - 1)P$ where $\alpha, \beta \in G(P)$. Then $C_\Omega(D,G)$ has minimum distance at least* $\deg G - (2g-2) + r$.

Proof. Let $P_1, \ldots, P_r$ be the extensions of P in the degree r constant field extension F' of F. By Proposition 2.4, $(\alpha, \ldots, \alpha), (\beta, \ldots, \beta) \in G_0(P_1, \ldots, P_r)$ as $\alpha, \beta \in G(P)$. Take $G' = Con_{F'/F}(G) = \sum_{i=1}^r (\alpha + \beta - 1)P_i$ and $D' = Con_{F'/F}(D)$ in Lemma 3.2. Then the minimum distance of $C_\Omega(D', G')$ satisfies

$$\begin{array}{rcl} d\left(C_\Omega(D', G')\right) & \geq & \deg G' - (2g-2) + r \\ & = & \deg G - (2g-2) + r. \end{array}$$

From Lemma 3.1 it follows that the minimum distance of $C_\Omega(D,G)$ is at least $\deg G - (2g-2) + r$. □

Next, we modify [2, Theorem 3.4] to obtain a result similar to [3, Theorem 4] for codes defined using places of higher degree.

Theorem 3.5. *Let P be a place of degree r and $Q_1, \ldots, Q_n$ be distinct places of $F/\mathbb{F}_q$ of degree one such that $Q_i \neq P$ for each i, $1 \leq i \leq n$. Set $D := Q_1 + \cdots + Q_n$. Suppose $G := (\alpha + (\alpha + t) - 1)P$ where $\alpha, \ldots, \alpha + t \in G(P)$ with $t \geq 0$. Then $C_\Omega(D,G)$ has minimum distance at least* $\deg G - (2g-2) + r(t+1)$.

Proof. Let $P_1, \dots, P_r$ be the extensions of P in the degree r constant field extension F' of F. By Proposition 2.4, $[\alpha, \alpha+t]^r \subseteq G_0(P_1, \dots, P_r)$ as $\alpha, \dots, \alpha+t \in G(P)$. Thus, $\mathbf{v} \in G_0(P_1, \dots, P_r)$ for all $\mathbf{v}$ such that $(\alpha, \dots, \alpha) \preceq \mathbf{v} \preceq (\alpha+t, \dots, \alpha+t)$. Take $G' = Con_{F'/F}(G) = \sum_{i=1}^{r}(\alpha+(\alpha+t)-1)P_i$ and $D' = Con_{F'/F}(D)$ in Lemma 3.3. Then the minimum distance of $C_\Omega(D', G')$ satisfies

$$\begin{aligned} d\left(C_\Omega(D', G')\right) &\geq \deg G' - (2g-2) + r + rt \\ &= \deg G - (2g-2) + r + rt. \end{aligned}$$

From Lemma 3.1 it follows that the minimum distance of $C_\Omega(D, G)$ is at least $\deg G - (2g-2) + r(t+1)$. □

Example 3.6. Consider the Hermitian function field $F := \mathbb{F}_{81}(x,y)/\mathbb{F}_{81}$ defined by $y^9 + y = x^{10}$. Note that F has genus 36 and 730 places of degree one. Using Magma [1], we find that F has a place P of degree 3 with Weierstrass gap set

$$G(P) = \{1, 2, 3, 4, 5, 6, 7, 11, 12, 13, 14, 20\}.$$

Take $\alpha = 14$ and $\beta = 20$ in the Theorem 3.4. Then

$$G := (14 + 20 - 1)P = 33P.$$

Let D be the sum of all places of F of degree one other than P_∞. Then $C_\Omega(D, G)$ is a $[729, 665, \geq 32]$ code. The one-point code on F of dimension 665 is a $[729, 665, 29]$-code. The gap set $G(P)$ may be used to construct several other codes which have greater minimum distance than the comparable one-point Hermitian code.

Example 3.7. Consider the Hermitian function field $F := \mathbb{F}_{49}(x,y)/\mathbb{F}_{49}$ defined by $y^7 + y = x^8$. Note that F has genus 21 and 344 places of degree one. Using Magma [1], we find that F has a place P of degree 3 with Weierstrass gap set

$$G(P) = \{1, 2, 3, 4, 5, 9, 10\}.$$

Take $\alpha = 9$ and $t = 1$ in the Theorem 3.5. Then

$$G := (9 + 10 - 1)P = 18P.$$

Let D be the sum of all places of F of degree one other than P_∞. Then $C_\Omega(D, G)$ is a $[343, 309, \geq 20]$ code. The one-point code on F of dimension 309 is a $[343, 309, 14]$-code. Note that the existence of an AG code on F with parameters $[343, 309, \geq 18]$ is shown in [9].

Example 3.8. Consider the Hermitian function field $F := \mathbb{F}_{64}(x,y)/\mathbb{F}_{64}$ defined by $y^8 + y = x^9$. Note that F has genus 28 and 513 places of degree one. Using Magma [1], we find that F has a place P of degree 3 with Weierstrass gap set

$$G(P) = \{1, 2, 3, 4, 5, 6, 10, 11, 12\}.$$

Take $\alpha = 10$ and $t = 2$ in the Theorem 3.5. Then

$$G := (10 + 12 - 1)P = 21P.$$

Let D be the sum of all places of F of degree one other than P_∞. Then $C_\Omega(D, G)$ is a $[512, 476, \geq 18]$ code. The one-point code on F of dimension 309 is a $[512, 476, 9]$-code. Hence, the code constructed using a place of higher degree corrects at least twice as many errors as the comparable one-point code from the same function field. It is worth pointing out that while there exists a $\mathbb{F}_{64}$-rational divisor G' of F such that $C_\Omega(D', G')$ is a $[512, 476, \geq 19]$-code [9], it is not clear how to determine G'.

Remark 3.9. While Theorem 3.4 and Theorem 3.5 may be thought of as prescribing a method for constructing one-point codes from places of higher degree, these results can also be viewed as specifying a method for defining r-point codes so that the results of [4], [2] apply.

4. Acknowledgements

The authors wish to thank A. Garcia and R. F. Lax for pointing out the reference [5]. Some of these results also appear in the second author's M. S. thesis [7].

References

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

[2] C. Carvalho and F. Torres, On Goppa codes and Weierstrass gaps at several points, Designs, Codes and Crypt., to appear.

[3] 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.

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

[5] J. Lewittes, Genus and gaps in function fields, J. Pure Appl. Algebra **58** (1989), 29–44.

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

[7] T. W. Michel, One-point codes using places of higher degree, M. S. thesis., Clemson University, 2004.

[8] H. Stichtenoth, Algebraic Function Fields and Codes, Springer-Verlag, 1993.

[9] 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.

[10] C. P. Xing, H. Niederreiter, and K. Y. Lam, A generalization of algebraic geometry codes, IEEE Trans. Inform. Theory **45** (1999), 2498–2501.