RIEMANN-ROCH SPACES OF THE HERMITIAN FUNCTION FIELD WITH APPLICATIONS TO ALGEBRAIC GEOMETRY CODES AND LOW-DISCREPANCY SEQUENCES

HIREN MAHARAJ[a], GRETCHEN L. MATTHEWS[b], & GOTTLIEB PIRSIC[c]

[a] DEPARTMENT OF MATHEMATICAL SCIENCES, CLEMSON UNIVERSITY, CLEMSON, SC 29634-0975 USA
HMAHARA@CLEMSON.EDU

[b] DEPARTMENT OF MATHEMATICAL SCIENCES, CLEMSON UNIVERSITY, CLEMSON, SC 29634-0975 USA
GMATTHE@CLEMSON.EDU

[c] JOHANN RADON INSTITUTE FOR COMPUTATIONAL AND APPLIED MATHEMATICS, AUSTRIAN ACADEMY OF SCIENCE, ALTENBERGERSTRASSE 69, A-4040 LINZ, AUSTRIA
GOTTLIEB.PIRSIC@OEAW.AC.AT

Abstract. This paper is concerned with two applications of bases of Riemann-Roch spaces. In the first application, we define the floor of a divisor and obtain improved bounds on the parameters of algebraic geometry codes. These bounds apply to a larger class of codes than that of Homma and Kim (Goppa codes with Weierstrass pairs, J. Pure Appl. Algebra **162** (2001), 273-290). Then we determine explicit bases for large classes of Riemann-Roch spaces of the Hermitian function field. These bases give better estimates on the parameters of a large class of m-point Hermitian codes. In the second application, these bases are used for fast implementation of Niederretier and Xing's method (A construction of low-discrepancy sequences using global function fields, Acta. Arith. **72** (1995), 281-298) for the construction of low-discrepancy sequences.

1. Introduction

This study is motivated by two primary applications: the construction of algebraic geometry codes and the construction of low-discrepancy

Key words and phrases. Riemann-Roch space, algebraic geometry code, low-discrepancy sequence.

* Corresponding author: Gretchen L. Matthews, phone: 864-656-5239, fax: 864-656-5230.

sequences. In both applications, it is useful to have explicit bases of certain Riemann-Roch spaces. In this paper we find such bases as well as a compact description of them for the Hermitian function field.

This paper is organized as follows. In Section 2, we introduce the notion of the *floor* of a divisor. Given a divisor G of a function field $F/\mathbb{F}_q$ with $\dim \mathcal{L}(G) > 0$, the *floor* of G is a divisor G' of F of minimum degree such that $\mathcal{L}(G) = \mathcal{L}(G')$. We show that the floor of a divisor exists and is unique. We also indicate how to find the floor of a given divisor G, denoted $\lfloor G \rfloor$. In this section, we also relate the notion of a floor of a divisor supported by m places $Q_1, \ldots, Q_m$ to the Weierstrass semigroup $H(Q_1, \ldots, Q_m)$ and the Weierstrass gap set $G(Q_1, \ldots, Q_m)$ of the m-tuple of places $(Q_1, \ldots, Q_m)$. Our main result in Section 2 is the following improved lower bound on the minimum distance of algebraic geometric codes:

Theorem 2.10 *Let $F/\mathbb{F}_q$ be a function field of genus g. Let $D := P_1 + \cdots + P_n$ where $P_1, \ldots, P_n$ are distinct rational places of F, and let $G := H + \lfloor H \rfloor$ be a divisor of F such that H is an effective divisor whose support does not contain any of the places $P_1, \ldots, P_n$. Set $E_H := H - \lfloor H \rfloor$. Then $C_\Omega(G, D)$ is an $[n, k, d]$ code whose parameters satisfy*

$$k \geq n - \deg G + g - 1$$

and

$$d \geq \deg G - (2g - 2) + \deg E_H = 2 \deg H - (2g - 2).$$

This bound is more general than those in [9], [4], and [11] which are obtained by using Weierstrass gap sets. We give specific examples (Example 2.7 and Example 2.11) to illustrate this theorem.

In Section 3, we restrict our attention to the Hermitian function field. Recall that the Hermitian function field $H = \mathbb{F}_{q^2}(x, y)$ is defined by

$$y^q + y = x^{q+1}.$$

The following are some basic facts about this function field.

Proposition 1.1. [15, Lemma VI.4.4]

(*a*) *The genus of H is $g = \frac{q(q-1)}{2}$.*

(*b*) *H has $q^3 + 1$ places of degree 1 over $\mathbb{F}_{q^2}$, namely*

- *the common pole Q_∞ of x and y, and*
- *for each $\alpha \in \mathbb{F}_{q^2}$, there are q elements $\beta \in \mathbb{F}_{q^2}$ such that $\beta^q + \beta = \alpha^{q+1}$, and for all such pairs (α, β) there is a unique place $P_{\alpha,\beta}$ of H of degree one with $x(P_{\alpha,\beta}) = \alpha$ and $y(P_{\alpha,\beta}) = \beta$.*

(*c*) *For $r \geq 0$, the elements $x^i y^j$ with $0 \leq i$, $0 \leq j \leq q - 1$, and $iq + j(q + 1) \leq r$ form a basis for the Riemann-Roch space $\mathcal{L}(rQ_\infty)$.*

In order to describe the results of Section 3, we set up the following notation. For $\alpha \in \mathbb{F}_{q^2}$, define

$$K_\alpha := \{\beta : \beta^q + \beta = \alpha^{q+1}\}$$

and

$$\mathcal{K} := \{(\alpha, \beta) \in \mathbb{F}_{q^2}^2 : \beta^q + \beta = \alpha^{q+1}\}.$$

For each $(\alpha, \beta) \in \mathcal{K}$, we define

$$\tau_{\alpha,\beta} := y - \beta - \alpha^q(x - \alpha).$$

In all that follows, whenever we write $\tau_{\alpha,\beta}$, it will be understood that $(\alpha, \beta) \in \mathcal{K}$. Note that $\tau_{\alpha,\beta}$ is the tangent line to the Hermitian curve at the point $(\alpha : \beta : 1)$. Let $\alpha \in \mathbb{F}_{q^2}$, $r \in \mathbb{Z}$, and $k_\beta \in \mathbb{Z}$ for each $\beta \in K_\alpha$. In Theorem 3.6 we show that the dimension of $\mathcal{L}(rQ_\infty + \sum_{\beta \in K_\alpha} k_\beta P_{\alpha,\beta})$ is given by

$$\sum_{i=0}^{q} \max\left\{ \left\lfloor \frac{r - iq}{q+1} \right\rfloor + \sum_{\beta \in K_\alpha} \left\lfloor \frac{k_\beta + i}{q+1} \right\rfloor + 1, 0 \right\}.$$

As a consequence of the proof of this dimension formula, it follows that the set of functions

$$\bigcup_{0 \le i \le q} \left\{ (x-\alpha)^i \prod_{\beta \in K_\alpha} \tau_{\alpha,\beta}^{e_{\beta,i}} : -\sum_{\beta \in K_\alpha} \left\lfloor \frac{k_\beta + i}{q+1} \right\rfloor \le \sum_{\beta \in K_\alpha} e_{\beta,i} \le \frac{r - iq}{q+1} \right\}$$

form a basis of the space $\mathcal{L}\left(rQ_\infty + \sum_{\beta \in K_\alpha} k_\beta P_{\alpha,\beta}\right)$. In Theorem 2.10, we use this fact to give a formula for the floor of the divisor $rQ_\infty + \sum_{\beta \in K_\alpha} k_\beta P_{\alpha,\beta}$.

Finally, in Section 4 we describe how to apply the above results in the construction of low-discrepancy sequences using the Niederreiter-Xing method on the Hermitian curve.

Notation Unless stated otherwise, we will use notation as in [15]. We write $F/\mathbb{F}_q$ to mean that F is an global function field with full field of constants $\mathbb{F}_q$. Let $g = g(F)$ denote the genus of F. If P is a rational place of F, that is, a place of degree one, then v_P denotes the discrete valuation corresponding to P. Given two divisors A, A' of F, the greatest common divisor of A and A' is

$$\gcd(A, A') := \sum_P \min\{v_P(A), v_P(A')\}P.$$

The support of a divisor A will be denoted by supp A. The divisor of a function $f \in F \setminus \{0\}$ (resp. differential $\eta \in \Omega \setminus \{0\}$, where Ω denotes the space of differentials of F) is denoted by (f) (resp. (η)). Given a divisor A of F, the Riemann-Roch space of A is the vector space

$\mathcal{L}(A) := \{f \in F : (f) \geq -A\} \cup \{0\}$ and the dimension of $\mathcal{L}(A)$ over $\mathbb{F}_q$ is denoted by $\ell(A)$. The vector space of differentials associated to A is $\Omega(A) := \{\eta \in \Omega : (\eta) \geq A\} \cup \{0\}$ and its dimension over $\mathbb{F}_q$ is denoted by $i(A)$.

Let $Q_1, \ldots, Q_m, P_1, \ldots, P_n$ be distinct rational places of F. Set $G := \sum_{i=1}^{m} \alpha_i Q_i$, where $\alpha_i \in \mathbb{Z}$ for all $1 \leq i \leq m$, and set $D := P_1 + \cdots + P_n$. We will consider the following two algebraic geometry codes defined using the divisors G and D:

$$C_{\mathcal{L}}(D, G) := \{(f(P_1), \ldots, f(P_n)) : f \in \mathcal{L}(G)\}$$

and

$$C_{\Omega}(D, G) := \{(res_{P_1}(\eta), \ldots, res_{P_n}(\eta)) : \eta \in \Omega(G - D)\}.$$

These two codes are sometimes referred to as m-point codes to indicate that there are m places in the support of the divisor G. It is well known that $C_{\mathcal{L}}(D, G)$ (resp. $C_{\Omega}(D, G)$) has length n (resp. n), dimension $\ell(G) - \ell(G - D)$ (resp. $i(G - D) - i(G)$), and minimum distance at least $n - \deg G$ (resp. at least $\deg G - (2g - 2)$).

2. Results for arbitrary function fields

Throughout this section, $F/\mathbb{F}_q$ denotes a global function field.

Proposition 2.1. *Let G be a divisor of a function field $F/\mathbb{F}_q$ with $\ell(G) > 0$. Suppose G' is a divisor of F of minimum degree such that $\mathcal{L}(G) = \mathcal{L}(G')$. Then $G \geq G'$. Consequently, G' is the unique divisor with respect to the above property.*

Proof: Since $\mathcal{L}(G) = \mathcal{L}(G') \cap \mathcal{L}(G) = \mathcal{L}(\gcd(G', G))$, it follows from the minimality of the degree of G' that $\deg G' \leq \deg \gcd(G', G)$. On the other hand $\gcd(G', G) \leq G'$. It follows that $G' = \gcd(G', G)$, whence $G' \leq G$.

Now suppose that G' and G'' are two divisors of F of minimum degree such that $\mathcal{L}(G') = \mathcal{L}(G) = \mathcal{L}(G'')$. From the above, the fact that G'' is a divisor of F of minimum degree such that $\mathcal{L}(G') = \mathcal{L}(G'')$ implies $G' \geq G''$. Similarly, $G'' \geq G'$ since G' is a divisor of F of minimum degree such that $\mathcal{L}(G'') = \mathcal{L}(G')$. Therefore, $G' = G''$. Hence, there is a unique divisor G' of F of minimum degree satisfying $\mathcal{L}(G) = \mathcal{L}(G')$. □

Definition 2.2. Given a divisor G of a function field $F/\mathbb{F}_q$ with $\ell(G) > 0$, the *floor* of G is the unique divisor G' of F of minimum degree such that $\mathcal{L}(G) = \mathcal{L}(G')$. The floor of G will be denoted by $\lfloor G \rfloor$.

Corollary 2.3. *Let G_1 and G_2 be divisors of a function field $F/\mathbb{F}_q$ with $\ell(G_1) > 0$ and $\ell(G_2) > 0$. Then $\mathcal{L}(G_1) = \mathcal{L}(G_2)$ if and only if $\lfloor G_1 \rfloor = \lfloor G_2 \rfloor$.*

PROOF: The forward implication follows from Proposition 2.1. Assume that $\lfloor G_1 \rfloor = \lfloor G_2 \rfloor$. Then $\mathcal{L}(G_1) = \mathcal{L}(\lfloor G_1 \rfloor) = \mathcal{L}(\lfloor G_2 \rfloor) = \mathcal{L}(G_2)$. □

The next three results will aid in searching for the floor of a divisor. The second of these is especially useful, because it implies that if a divisor G is effective and supp $G \cap$ supp $D = \emptyset$, then supp $\lfloor G \rfloor \cap$ supp $D = \emptyset$.

Proposition 2.4. *Let G be a divisor of $F/\mathbb{F}_q$ with $\ell(G) > 0$. Define the effective divisor $E := \gcd(G+(x) : x \in \mathcal{L}(G)\backslash\{0\})$. Then $\lfloor G \rfloor = G - E$.*

PROOF: Observe that for any place P, we have

$$\min_{x \in \mathcal{L}(G)\backslash\{0\}} v_P(x) = -v_P(G - E).$$

Then for any $f \in \mathcal{L}(G) \setminus \{0\}$, $v_P(f) \geq -v_P(G - E)$, whence $f \in \mathcal{L}(G - E)$. Thus, $\mathcal{L}(G) \subseteq \mathcal{L}(G - E)$. Since $G - E \leq G$, we also have $\mathcal{L}(G - E) \subseteq \mathcal{L}(G)$. Hence, $\mathcal{L}(G - E) = \mathcal{L}(G)$. By Proposition 2.1, we have $G - E \geq \lfloor G \rfloor$. Suppose that there is a place P such that $v_P(G - E) > v_P(\lfloor G \rfloor)$. Then $G - E > G - E - P \geq \lfloor G \rfloor$, and so

$$\mathcal{L}(G) = \mathcal{L}(\lfloor G \rfloor) \subseteq \mathcal{L}(G - E - P) \subseteq \mathcal{L}(G - E).$$

Since $\mathcal{L}(G) = \mathcal{L}(G - E)$, it follows that $\mathcal{L}(G - E) = \mathcal{L}(G - E - P)$. By the definition of E, there exists $x \in \mathcal{L}(G) = \mathcal{L}(G - E)$ such that $v_P(x) = -v_P(G - E)$. Clearly, $x \notin \mathcal{L}(G - E - P)$ which is a contradiction. Therefore, $v_P(G - E) = v_P(\lfloor G \rfloor)$ for all places P of F, and so $G - E = \lfloor G \rfloor$. □

Theorem 2.5. *If G is an effective divisor of $F/\mathbb{F}_q$, then $\lfloor G \rfloor$ is also effective. In particular, if G is effective, then the support of $\lfloor G \rfloor$ is a subset of the support of G.*

PROOF: Since G is effective, the constant functions belong to $\mathcal{L}(G)$. It follows that

$$v_P(G) \geq v_P(\lfloor G \rfloor) = -\min_{x \in \mathcal{L}(G)\backslash\{0\}} v_P(x) \geq 0$$

for any place P of F. □

Theorem 2.6. *Let G be a divisor of $F/\mathbb{F}_q$ and let $b_1, \ldots, b_t \in \mathcal{L}(G)$ be a spanning set for $\mathcal{L}(G)$. Then*

$$\lfloor G \rfloor = -\gcd((b_i) : i = 1, \ldots, t).$$

PROOF: Let $E = \gcd(G + (x) : x \in \mathcal{L}(G) \setminus \{0\})$. Then, since any $x \in \mathcal{L}(G) \setminus \{0\}$ is a nontrivial linear combination of the b_i, $G + (x) \geq \gcd(G + (b_i) : i = 1, \ldots, t)$. This implies that

$$E = \gcd(G + (b_i) : i = 1, \ldots, t).$$

Thus

$$\begin{aligned} \lfloor G \rfloor &= G - E \\ &= G - \gcd(G + (b_i) : i = 1, \ldots, t) \\ &= -\gcd((b_i) : i = 1, \ldots, t). \end{aligned}$$

□

Example 2.7. Consider the function field $F := \mathbb{F}_8(x, y)/\mathbb{F}_8$ with defining equation

$$y^8 - y = x^{10} - x^3.$$

This function field is sometimes referred to as the Suzuki function field over $\mathbb{F}_8$. It is easy to check that F has 65 rational places consisting of all places $P_{\alpha,\beta}$ where $\alpha, \beta \in \mathbb{F}_8$ and the infinite place P_∞.

We will illustrate how Theorem 2.6 may be used to find the floor of a divisor. Let

$$G := 14P_\infty + 11P_{0,0}.$$

In order to apply Theorem 2.6, we must have a spanning set for $\mathcal{L}(G)$. In most cases, determining such a set is nontrivial (hence the advantage of Theorem 3.3 in the Hermitian case). However, one can check that the set

$$B := \left\{1, x, y, v, w, \frac{v}{w}, \frac{y}{w}, \frac{x^2}{w}, \frac{xy}{w}, \frac{y^2}{w}, \frac{vy}{w}, \frac{v^2}{w}\right\},$$

where $v := y^4 - x^5$ and $w := y^4x - v^4$ is a basis of $\mathcal{L}(G)$ (see Lemma 3.5). According to Theorem 2.6 and Theorem 2.5,

$$\lfloor G \rfloor = -\gcd(v_{P_\infty}(b)P_\infty + v_{P_{0,0}}(b)P_{0,0} : b \in B).$$

One can then compute that

$$\begin{aligned} \lfloor G \rfloor &= -\min\{0, -8, -10, -12, -13, 1, 3, -3, -5, -7, -9, -11\}\, P_\infty \\ &\quad -\min\{0, 1, 3, 5, 13, -8, -10, -11, -9, -7, -5, -3\}\, P_{0,0} \\ &= 13P_\infty + 11P_{0,0}. \end{aligned}$$

Remark 2.8. Let $(n_1, \ldots, n_m) \in \mathbb{N}_0$, where $\mathbb{N}_0$ denotes the set of non-negative integers. Suppose $Q_1, \ldots, Q_m$ are distinct rational places of $F/\mathbb{F}_q$. Recall that $(n_1, \ldots, n_m)$ is an element of the Weierstrass semigroup of the m-tuple of places $(Q_1, \ldots, Q_m)$ if and only if

$$\ell\left(\sum_{i=1}^{m} n_i Q_i\right) = \ell\left((n_j - 1)Q_j + \sum_{i=1,\, i\neq j}^{m} n_i Q_i\right) + 1$$

for all $1 \leq j \leq m$. The complement of the Weierstrass semigroup of the m-tuple above is called the Weierstrass gap set of the m-tuple, denoted $G(Q_1, \ldots, Q_m)$. Hence, $(n_1, \ldots, n_m)$ is an element of the Weierstrass gap set of the m-tuple of places $(Q_1, \ldots, Q_m)$ if and only if there exists $j, 1 \leq j \leq m$, such that

$$\ell\left(\sum_{i=1}^{m} n_i Q_i\right) = \ell\left((n_j - 1)Q_j + \sum_{i=1,\, i\neq j}^{m} n_i Q_i\right). \tag{1}$$

While the Weierstrass gap set of a single place is a classically studied object, the Weierstrass gap set of an m-tuple of places was defined in [1] for $m = 2$ and in [2] for $m \geq 2$.

Based on these definitions, it is not surprising that there is a connection between the Weierstrass semigroup of the m-tuple $(Q_1, \ldots, Q_m)$ and floors of divisors supported by the places $Q_1, \ldots, Q_m$. It is easy to see that if $G = \sum_{i=1}^{m} \alpha_i Q_i$ is an effective divisor supported by m distinct rational places, then $\lfloor G \rfloor = G$ if and only if $(\alpha_1, \ldots, \alpha_m)$ is an element of the Weierstrass semigroup of the m-tuple $(Q_1, \ldots, Q_m)$.

The main motivation for studying the notion of the floor of a divisor is that it leads to improved estimates of the minimum distance of algebraic geometric codes. The first of these improved estimates follows immediately from the definition of the floor of a divisor. Recall that given a divisor G, $\deg G \geq \deg \lfloor G \rfloor$.

Theorem 2.9. *Let $F/\mathbb{F}_q$ be a function field of genus g. Let $D := P_1 + \cdots + P_n$ where $P_1, \ldots, P_n$ are distinct rational places of F, and let G be a divisor of F such that the support of $\lfloor G \rfloor$ does not contain any of the places $P_1, \ldots, P_n$. Then $C_{\mathcal{L}}(G, D)$ is an $[n, k, d]$ code whose parameters satisfy*

$$k \geq \deg G - g + 1$$

and

$$d \geq n - deg \lfloor G \rfloor.$$

Notice that Theorem 2.9 provides a generalization of [7, Theorem 3]. While the notion of the floor of a divisor is clearly inspired by the definition of the code $C_{\mathcal{L}}(D, G)$, the floor may also be used to study codes of the form $C_{\Omega}(D, G)$. This is detailed in the following discussion.

In [9] and [4], elements of the Weierstrass gap set satisfying (1) for all j, $1 \leq j \leq m$, are considered. These elements of the Weierstrass gap set have additional "symmetry" and are known as pure gaps. In particular, Homma and Kim define the pure gap set of a pair of points (Q_1, Q_2) to consist of those elements (α_1, α_2) of the Weierstrass gap set of the pair (Q_1, Q_2) with the following "symmetry" property: the

pairs (α_1', α_2) and (α_1, α_2') are elements of the Weierstrass gap set of the pair (Q_1, Q_2) for all $0 \leq \alpha_1' \leq \alpha_1$ and $0 \leq \alpha_2' \leq \alpha_2$ [9]. We note that this notion of symmetry agrees with that mentioned above. They obtain an improved lower bound on the minimum distance of certain algebraic geometry codes of the form $C_\Omega(D, \alpha_1 Q_1 + \alpha_2 Q_2)$ constructed using pure gaps of the pair (Q_1, Q_2). This is generalized in [4] to codes of the form $C_\Omega(D, \sum_{i=1}^m \alpha_i Q_i)$, $m \geq 2$, using the pure gap set of the m-tuple $(Q_1, \ldots, Q_m)$.

The following theorem shows how the usual lower bound may be improved in a more general situation, that is, a situation where the "symmetry" required in [9] and [4] is not necessarily present. Both [9, Theorem 3.3] and [4, Theorem 3.4] are special cases of the next result. In addition, we recover a corollary of [7, Theorem 4] which is typically applied to one-point codes.

Theorem 2.10. *Let $F/\mathbb{F}_q$ be a function field of genus g. Let $D := P_1 + \cdots + P_n$ where $P_1, \ldots, P_n$ are distinct rational places of F, and let $G := H + \lfloor H \rfloor$ be a divisor of F such that H is an effective divisor whose support does not contain any of the places $P_1, \ldots, P_n$. Set $E_H := H - \lfloor H \rfloor$. Then $C_\Omega(G, D)$ is an $[n, k, d]$ code whose parameters satisfy*

$$k \geq n - \deg G + g - 1$$

and

$$d \geq \deg G - (2g - 2) + \deg E_H = 2 \deg H - (2g - 2).$$

PROOF: The dimension estimate is clear. Choose $\eta \in \Omega(G - D)$ such that the codeword $c := (\mathrm{res}_{P_1}(\eta), \ldots, \mathrm{res}_{P_n}(\eta))$ is of minimum weight. We may assume that the first d coordinates of c are nonzero and that the remaining coordinates are zero. Then, putting $D' := \sum_{i=1}^d P_i$, we have $(\eta) \geq G - D'$ so that there is an effective divisor A whose support does not contain $P_1, \ldots, P_d$ such that $(\eta) = G - D' + A$. Taking degrees on both sides we have $2g - 2 = \deg G - d + \deg A$. Therefore,

$$d = \deg G - (2g - 2) + \deg A.$$

In order to prove the claimed minimum distance bound, it suffices to show that $\deg A \geq \deg E_H$.

Observe that

$$\deg A \geq \ell(H + A) - \ell(H) = \ell(H + A) - \ell(\lfloor H \rfloor) \geq \ell(H + A) - \ell(\lfloor H \rfloor + A).$$

We show that $\deg E_H = \ell(H + A) - \ell(\lfloor H \rfloor + A)$. Using the fact that $W := G - D' + A$ is a canonical divisor, we have by the Riemann-Roch theorem that

$$\begin{aligned}\ell(H+A)-\ell(\lfloor H\rfloor+A) &= \deg E_H+\ell(W-H-A)-\ell(W-\lfloor H\rfloor-A)\\ &= \deg E_H+\ell(\lfloor H\rfloor-D')-\ell(H-D').\end{aligned}$$

To complete the proof, we show that $\mathcal{L}(\lfloor H\rfloor - D') = \mathcal{L}(H-D')$. Observe that $\mathcal{L}(H-D') \subseteq \mathcal{L}(H) = \mathcal{L}(\lfloor H\rfloor)$, whence $\mathcal{L}(H-D') = \mathcal{L}(H-D')\cap\mathcal{L}(\lfloor H\rfloor) = \mathcal{L}(\gcd(H-D',\lfloor H\rfloor))$. By assumption, supp $H\cap$ supp $D=\emptyset$, so $\gcd(H-D',\lfloor H\rfloor) = \lfloor H\rfloor - D'$. This implies that $\mathcal{L}(\lfloor H\rfloor - D') = \mathcal{L}(\gcd(H-D',\lfloor H\rfloor)) = \mathcal{L}(H-D')$. It follows that

$$d = \deg G-(2g-2)+\deg A \geq \deg G-(2g-2)+\deg E_H.$$

□

Example 2.11. As in Example 2.7, let $F/\mathbb{F}_8$ denote the function field with defining equation

$$y^8-y = x^{10}-x^3.$$

Then the genus of F is $g=14$. Let us consider the code $C_\Omega(D, 27P_\infty + 22P_{0,0})$ where $D := P_1+\cdots+P_{63}$ is the sum of all rational places of F other than P_∞ and $P_{0,0}$. Set

$$G := 27P_\infty + 22P_{0,0}.$$

In order to apply Theorem 2.10, we must find a divisor H of F such that $H+\lfloor H\rfloor = 27P_\infty+22P_{0,0}$. According to Example 2.7, we can take

$$H = 14P_\infty + 11P_{0,0}$$

so that

$$H+\lfloor H\rfloor = (14P_\infty+11P_{0,0})+(13P_\infty+11P_{0,0}) = G.$$

Then, by applying Theorem 2.10, we see that $C_\Omega(D,G)$ is a code of length 63, dimension 27, and minimum distance at least 24. This is the best known code over $\mathbb{F}_8$ of length 63 and dimension 27 (cf. [3]). We note that this code originally appeared in a preprint by the second author. Also, codes defined using the Suzuki function field were considered first in [8]. Such codes were studied more recently in [5] and the above mentioned preprint where a number of codes are given with parameters better than the best known code of the same length and dimension (according to [3]). It is worth noting that while there exists a $[64, 28, 24]$ one-point code [5], the two-point code mentioned above cannot be obtained by shortening this one-point code. One may also notice that [9, Theorem 3.3] and [4, Theorem 3.4] cannot be applied to this code.

3. Applications to the Hermitian function field

In this section, we will restrict our attention to the Hermitian function field $H = \mathbb{F}_{q^2}(x, y)/\mathbb{F}_{q^2}$ with defining equation $y^q + y = x^{q+1}$. We recall some notation from the introduction. Let

$$\mathcal{K} := \{(\alpha, \beta) \in \mathbb{F}_{q^2}^2 : \beta^q + \beta = \alpha^{q+1}\}.$$

For each $\alpha \in \mathbb{F}_{q^2}$, let

$$K_\alpha := \{\beta : \beta^q + \beta = \alpha^{q+1}\},$$

and for each $(\alpha, \beta) \in \mathcal{K}$, set

$$\tau_{\alpha,\beta} := y - \beta - \alpha^q(x - \alpha).$$

Throughout this section, α is a fixed element of $\mathbb{F}_{q^2}$ and r and k_β (for each $\beta \in K_\alpha$) are fixed integers. If one views H as a Kummer extension over $\mathbb{F}_{q^2}(y)$, the rational places of $\mathbb{F}_{q^2}(y)$ behave as follows:

- For each $\gamma \in \mathbb{F}_{q^2}$ such that $\gamma^q + \gamma = 0$, the place $y - \gamma$ is totally ramified. If $\gamma^q + \gamma \neq 0$, the place $y - \gamma$ splits completely in H.
- The pole of y is totally ramified.

For our purposes, we define the Kummer extension H as follows. Observe that

$$\tau_{\alpha,\beta}^q + \tau_{\alpha,\beta} = (x - \alpha)^{q+1}. \tag{2}$$

Then $H = \mathbb{F}_{q^2}(x, y) = \mathbb{F}_{q^2}(\tau_{\alpha,\beta}, x)$. Moreover, the divisor of $\tau_{\alpha,\beta}$ is

$$(\tau_{\alpha,\beta}) = (q + 1)P_{\alpha,\beta} - (q + 1)Q_\infty.$$

Following the usual convention for rational function fields, we denote the places of $\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$ by their corresponding monic irreducible polynomials, except in the case of the place at infinity which we denote by $P_\infty(\tau_{\alpha,\beta})$. For any $\gamma \in \mathbb{F}_{q^2}$ satisfying $\gamma^q + \gamma = 0$, we have $\tau_{\alpha,\beta} - \gamma = \tau_{\alpha,\beta+\gamma}$. Thus, we will write "the place $\tau_{\alpha,\beta+\gamma}$ in $\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$" to mean the place $\tau_{\alpha,\beta} - \gamma$. Viewing H as an extension of $\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$, we have the following result, which we record for reference purposes.

Lemma 3.1. *Let $H/\mathbb{F}_{q^2}$ denote the Hermitian function field, and let $\gamma \in \mathbb{F}_{q^2}$.*

(a) If $\gamma^q + \gamma = 0$, the place $\tau_{\alpha,\beta} - \gamma = \tau_{\alpha,\beta+\gamma}$ in $\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$ is totally ramified in the extension $H/\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$.

(b) If $\gamma^q + \gamma \neq 0$, the place $\tau_{\alpha,\beta} - \gamma$ in $\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$ splits completely in the extension $H/\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$.

(c) The pole $P_\infty(\tau_{\alpha,\beta})$ of $\tau_{\alpha,\beta}$ is totally ramified in the extension $H/\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$.

Lemma 3.2. *The functions* 1, $x-\alpha$, $(x-\alpha)^2$, ..., $(x-\alpha)^q$ *form an integral basis of the Hermitian function field* $H/\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$ *at any place* P *of* $\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$ *different from* $P_\infty(\tau_{\alpha,\beta})$.

PROOF: Let P be any place of $H/\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$ such that $P \neq P_\infty(\tau_{\alpha,\beta})$. The minimum polynomial of $x-\alpha$ over $\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$ is $\phi(T) = T^{q+1} - (\tau_{\alpha,\beta}^q + \tau_{\alpha,\beta})$. Let R be any place of H which lies above P. According to [15, Theorem III.5.10(b)], we must show that $v_R(\phi'(x-\alpha)) = d(R|P)$. Now $v_R(\phi'(x-\alpha)) = qv_R(x-\alpha)$. If $R = P_{\alpha,\gamma}$ for some $\gamma \in K_\alpha$, then $d(R|P) = e(R|P) - 1 = q$ and $v_R(x-\alpha) = 1$, so that $v_R(\phi'(x-\alpha)) = d(R|P)$. If $R \neq P_{\alpha,\gamma}$ for any $\gamma \in K_\alpha$, then $v_R(x-\alpha) = 0 = d(R|P)$ since R is unramified over P. Therefore $\{1, x-\alpha, (x-\alpha)^2, \ldots, (x-\alpha)^q\}$ is an integral basis of $H/\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$ at P. □

Theorem 3.3. *Consider the Hermitian function field* $H/\mathbb{F}_{q^2}$ *and the divisor* $rQ_\infty + \sum_{\beta\in K_\alpha} k_\beta P_{\alpha,\beta}$ *of* H *where* $\alpha \in \mathbb{F}_{q^2}$, $r \in \mathbb{Z}$, *and* $k_\beta \in \mathbb{Z}$ *for each* $\beta \in K_\alpha$. *Set*

$$S := \left\{ (x-\alpha)^i \prod_{\beta\in K_\alpha} \tau_{\alpha,\beta}^{e_{\beta,i}} : \begin{array}{l} e_{\beta,i} \in \mathbb{Z}, -k_\beta \le e_{\beta,i}(q+1)+i, \text{ and} \\ (q+1)\sum_{\beta\in K_\alpha} e_{\beta,i} + iq \le r \ \forall i, 0 \le i \le q \end{array} \right\}.$$

Then $\mathcal{L}(rQ_\infty + \sum_{\beta\in K_\alpha} k_\beta P_{\alpha,\beta})$ *is the* $\mathbb{F}_{q^2}$*-linear span of* S.

PROOF: Let $\mathcal{L} := \mathcal{L}(rQ_\infty + \sum_{\beta\in K_\alpha} k_\beta P_{\alpha,\beta})$. It is readily checked that $S \subseteq \mathcal{L}$ as

$$\left((x-\alpha)^i \prod_{\beta\in K_\alpha} \tau_{\alpha,\beta}^{e_{\beta,i}} \right) = \sum_{\beta\in K_\alpha} (e_{\beta,i}(q+1)+i)P_{\alpha,\beta} - ((q+1)\sum_{\beta\in K_\alpha} e_{\beta,i} + iq)Q_\infty.$$

Fix $\beta \in K_\alpha$. Let $z \in \mathcal{L}$. Then Q_∞ and the places $P_{\alpha,\delta}$ ($\delta \in K_\alpha$) are the only possible poles of z. Thus, by Lemma 3.2, there exist $z_i \in \mathbb{F}_{q^2}(\tau_{\alpha,\beta})$ such that

$$z = z_0 + z_1(x-\alpha) + \cdots + z_q(x-\alpha)^q$$

and the only possible poles in $\mathbb{F}_{q^2}(\tau_{\alpha,\beta})$ of the z_i are $P_\infty(\tau_{\alpha,\beta})$ and the places $\tau_{\alpha,\delta}$ where $\delta \in K_\alpha$. It follows that the z_i are of the form

$$z_i = g_i(\tau_{\alpha,\beta}) \prod_{\delta\in K_\alpha} \tau_{\alpha,\delta}^{e_{\delta,i}} \tag{3}$$

where the $e_{\beta,i}$ are integers, $g_i(\tau_{\alpha,\beta})$ is polynomial in $\tau_{\alpha,\beta}$, and $\tau_{\alpha,\delta}$ does not divide $g_i(\tau_{\alpha,\beta})$ for any $\delta \in K_\alpha$. Thus, z_i is an $\mathbb{F}_{q^2}$-linear combination of the functions

$$A_{i,j} := \tau_{\alpha,\beta}^j \prod_{\delta\in K_\alpha} \tau_{\alpha,\delta}^{e_{\delta,i}} \tag{4}$$

for $j = 0, 1, \ldots, \deg g_i$. In order to prove the theorem, we show that for $0 \leq i \leq q$ and $j = 0, \ldots, \deg g_i$, the functions $(x-\alpha)^i A_{i,j}$ belong to S. Note that

$$(x-\alpha)^i A_{i,j} = (x-\alpha)^i \tau_{\alpha,\beta}^{e_{\beta,i}+j} \prod_{\delta \in K_\alpha \setminus \{\beta\}} \tau_{\alpha,\beta}^{e_{\delta,i}}.$$

Hence, for $0 \leq i \leq q$ and $0 \leq j \leq \deg g_i$,we must show that

$$(q+1)(e_{\beta,i}+j) + i \geq -k_\beta, \tag{5}$$

$$(q+1)e_{\delta,i} + i \geq -k_\delta, \tag{6}$$

for $\delta \in K_\alpha \setminus \{\beta\}$, and

$$(q+1)\left(j + \sum_{\delta \in K_\alpha} e_{\delta,i}\right) + iq \leq r. \tag{7}$$

Let $\delta_0 \in K_\alpha$ and put $P := P_{\alpha,\delta_0}$ and $\tau := \tau_{\alpha,\delta_0}$. By Lemma 3.1, we have

$$v_P(z_i(x-\alpha)^i) = (q+1)v_\tau(z_i) + i$$

as $z_i \in \mathbb{F}_{q^2}(\tau_{\alpha\delta_0}) = \mathbb{F}_{q^2}(\tau_{\alpha\beta})$ and $x - \alpha \in H$. From this, it follows that $v_P(z_i(x-\alpha)^i)$ are distinct modulo $q+1$ for $0 \leq i \leq q$. Hence, we have

$$v_P(z) = \min\{(q+1)v_\tau(z_i) + i : 0 \leq i \leq q\} \geq -k_{\delta_0}$$

since $z \in \mathcal{L}$. Thus for $0 \leq i \leq q$,

$$(q+1)v_\tau(z_i) + i \geq -k_{\delta_0}. \tag{8}$$

From (3) we have that

$$v_\tau(z_i) = e_{\delta_0,i} + v_\tau(g_i(\tau_{\alpha,\beta})) = e_{\delta_0,i},$$

so (8) becomes

$$(q+1)e_{\delta_0,i} + i \geq -k_{\delta_0} \tag{9}$$

for $0 \leq i \leq q$. Now, observe that for $j = 0, 1, \ldots, \deg g_i$,

$$(q+1)(e_{\beta,i}+j) + i \geq (q+1)e_{\beta,i} + i \geq -k_\beta. \tag{10}$$

We have proved (5) and (6). It remains for us to prove (7).

Put $Q := Q_\infty$ and $\infty := P_\infty(\tau_{\alpha,\beta})$. Then we have

$$v_Q(z_i(x-\alpha)^i) = (q+1)v_\infty(z_i) - iq = (q+1)(v_\infty(z_i)) - i) + i$$

which are distinct modulo $q+1$ for $0 \leq i \leq q$. Hence

$$v_Q(z) = \min\{(q+1)v_\infty(z_i) - iq : 0 \leq i \leq q\} \geq -r. \tag{11}$$

Thus, we have for $0 \leq i \leq q$,

$$(q+1)v_\infty(z_i) - iq \geq -r. \tag{12}$$

From (3) we have that

$$v_\infty(z_i) = -\left(\deg g_i + \sum_{\delta \in K_\alpha} e_{\delta,i}\right) \tag{13}$$

so that for $0 \leq i \leq q$, (12) becomes

$$(q+1)\left(\deg g_i + \sum_{\delta \in K_\alpha} e_{\delta,i}\right) + iq \leq r. \tag{14}$$

Now, observe that for $j = 0, 1, \ldots, \deg g_i$,

$$(q+1)\left(j + \sum_{\delta \in K_\alpha} e_{\delta,i}\right) + iq \leq (q+1)\left(\deg g_i + \sum_{\delta \in K_\alpha} e_{\delta,i}\right) + iq \leq r. \tag{15}$$

This proves (7) and completes the proof of the theorem. □

Corollary 3.4. *Consider the divisor $rQ_\infty + kP_{\alpha,\beta}$ of the Hermitian function field $H/\mathbb{F}_{q^2}$ where $\beta \in K_\alpha$ and $r, k \in \mathbb{Z}$. Let*

$$S := \left\{ (x-\alpha)^i \tau_{\alpha,\beta}^{e_i} : \begin{array}{l} e_i \in \mathbb{Z}, -k \leq e_i(q+1) + i, \text{ and} \\ (q+1)e_i + iq \leq r \ \forall i, 0 \leq i \leq q \end{array} \right\}.$$

Then S is an $\mathbb{F}_{q^2}$-basis for $\mathcal{L}(rQ_\infty + kP_{\alpha,\beta})$.

Proof: This follows from Theorem 3.3 since the elements of S have distinct valuations at the place Q_∞ and so are $\mathbb{F}_{q^2}$-linearly independent. □

The next lemma will be helpful in extracting bases for the space $\mathcal{L}(rQ_\infty + \sum_{\beta \in K_\alpha} k_\beta P_{\alpha,\beta})$ from the spanning set S given in Theorem 3.3.

Lemma 3.5. *Let $F/\mathbb{F}_q$ be a function field. Let G be a divisor of F and let P be a rational place of F. Let $V = \{v_P(z) : z \in \mathcal{L}(G) \setminus \{0\}\}$. For each $i \in V$, choose $u_i \in \mathcal{L}(G)$ such that $v_P(u_i) = i$. Then the set $B = \{u_i : i \in V\}$ is a basis for $\mathcal{L}(G)$.*

Proof: It is clear that the functions in B are $\mathbb{F}_q$-linearly independent. Let $z \in \mathcal{L}(G)$. We will show that z is in the linear span of the set B. If $z = 0$, then we are done. Assume that $z \neq 0$. Then there exists i_0 such that $v_P(z) = v_P(u_{i_0})$. Choose $a_0 \in \mathbb{F}_q$ such that $v_P(z - a_0 u_{i_0}) > v_P(z)$. If $z - a_0 u_{i_0} = 0$, we are done. Otherwise, we can choose $a_1 \in \mathbb{F}_q$ and i_1 such that $v_P(z - a_0 u_{i_0} - a_1 u_{i_1}) > v_P(z - a_0 u_{i_0})$. We continue in this way. Since B is a finite set, this process will stop, in which case we obtain the desired result. □

Theorem 3.6. *Consider the Hermitian function field $H/\mathbb{F}_{q^2}$ and the divisor $G := rQ_\infty + \sum_{\beta \in K_\alpha} k_\beta P_{\alpha,\beta}$ of H where $\alpha \in \mathbb{F}_{q^2}$, $r \in \mathbb{Z}$, and $k_\beta \in \mathbb{Z}$ for each $\beta \in K_\alpha$. The dimension of the space $\mathcal{L}(G)$ is given by*

$$\begin{aligned} \ell(G) &= \sum_{i=0}^{q} \max\left\{ \left\lfloor \tfrac{r-iq}{q+1} \right\rfloor + \sum_{\beta \in K_\alpha} \left\lfloor \tfrac{k_\beta + i}{q+1} \right\rfloor + 1, 0 \right\} \\ &\leq r + \sum_{\beta \in K_\alpha} k_\beta + 1. \end{aligned}$$

Proof: Set $\mathcal{L} := \mathcal{L}(rQ_\infty + \sum_{\beta \in K_\alpha} k_\beta P_{\alpha,\beta})$. For each $0 \leq i \leq q$, let

$$V_i := \left\{ -(q+1) \sum_{\beta \in K_\alpha} e_\beta - iq : \begin{array}{l} e_\beta \in \mathbb{Z}, -k_\beta \leq e_\beta(q+1) + i, \text{ and} \\ (q+1)\sum_{\beta \in K_\alpha} e_\beta + iq \leq r \ \forall \beta \in K_\alpha \end{array} \right\}$$

and let $V := \cup_{i=0}^{q} V_i$. The proof relies on two claims which are outlined below.

Claim 1: $V = \{v_{Q_\infty}(z) : z \in \mathcal{L} \setminus \{0\}\}$.

Proof of Claim 1: If $z \in \mathcal{L} \setminus \{0\}$, then it follows (from (11), (13), (14) and (9)) that $v_{Q_\infty}(z) \in V_i$ for some $0 \leq i \leq q$. Thus, $\{v_{Q_\infty}(z) : z \in \mathcal{L} \setminus \{0\}\} \subseteq V$. To complete the proof of Claim 1, it remains to verify that $V \subseteq \{v_{Q_\infty}(z) : z \in \mathcal{L} \setminus \{0\}\}$. Now let $m \in V$. Then $m \in V_j$ for some $0 \leq j \leq q$. Hence, there are integers e_β, where $\beta \in K_\alpha$, such that

$$m = -(q+1) \sum_{\beta \in K_\alpha} e_\beta - jq,$$

$(q+1)\sum_{\beta \in K_\alpha} e_\beta + jq \leq r$, and $-k_\beta \leq e_\beta(q+1) + j$ for all $\beta \in K_\alpha$. Observe that $v_{Q_\infty}(z) = m$ where

$$z = (x-\alpha)^j \prod_{\beta \in K_\alpha} \tau_{\alpha,\beta}^{e_\beta}$$

and that $z \in \mathcal{L}$. This concludes the proof of Claim 1.

According to Lemma 3.5, it follows that $\dim \mathcal{L} = |V|$. Therefore, we proceed to count the number of elements of V. To do so, we establish the following claim.

Claim 2: Fix i, $0 \leq i \leq q$. Then $-iq - c(q+1) \in V$ if and only if

$$-\sum_{\beta \in K_\alpha} \left\lfloor \frac{k_\beta + i}{q+1} \right\rfloor \leq c \leq \frac{r - iq}{q+1}.$$

Proof of Claim 2: Observe that for any integer N, there are unique integers a and b, with $0 \leq a \leq q$ such that $N = aq + (q+1)b$. This follows from the fact that the $q+1$ numbers N, $N-q$, $N-2q$, …, $N-q^2$ are distinct modulo $q+1$ so there is a unique a $(0 \leq a \leq q)$ such that $N - aq \equiv 0 \bmod q+1$. Hence, the sets V_i are mutually disjoint.

Thus, $-iq - c(q+1) \in V$ if and only if $-iq - c(q+1) \in V_i$. This holds if and only if there exist integers e_β ($\beta \in K_\alpha$) such that

$$-c(q+1) - iq = -(q+1) \sum_{\beta \in K_\alpha} e_\beta - iq,$$

$(q+1)\sum_{\beta \in K_\alpha} e_\beta + iq \leq r$, and $-k_\beta \leq (q+1)e_\beta + i$ for all $\beta \in K_\alpha$. Thus $-iq - c(q+1) \in V$ if and only if there exist integers e_β ($\beta \in K_\alpha$) such that

$$c = \sum_{\beta \in K_\alpha} e_\beta,$$

$(q+1)\sum_{\beta \in K_\alpha} e_\beta + iq \leq r$, and $(q+1)e_\beta + i \geq -k_\beta$ for all $\beta \in K_\alpha$ $(*)$. Clearly, the inequalities $(*)$ are equivalent to

$$-\sum_{\beta \in K_\alpha} \frac{k_\beta + i}{q+1} \leq \sum_{\beta \in K_\alpha} e_\beta \leq \frac{r - iq}{q+1}$$

and

$$e_\beta \geq \left\lceil -\frac{k_\beta + i}{q+1} \right\rceil = -\left\lfloor \frac{k_\beta + i}{q+1} \right\rfloor$$

for all $\beta \in K_\alpha$. Thus the desired integers e_β exist if and only if

$$-\sum_{\beta \in K_\alpha} \left\lfloor \frac{k_\beta + i}{q+1} \right\rfloor \leq c \leq \frac{r - iq}{q+1},$$

completing the proof of Claim 2.

Now it follows that $|V_i|$ is the number of integers in the interval $\left[-\sum_{\beta \in K_\alpha} \left\lfloor \frac{k_\beta + i}{q+1} \right\rfloor, \lfloor \frac{r-iq}{q+1} \rfloor\right]$; that is,

$$|V_i| = \max\left\{ \left\lfloor \frac{r - iq}{q+1} \right\rfloor + \sum_{\beta \in K_\alpha} \left\lfloor \frac{k_\beta + i}{q+1} \right\rfloor + 1, 0 \right\}.$$

Since the V_i's are mutually disjoint, this completes the proof. □

Corollary 3.7. *Consider the Hermitian function field $H/\mathbb{F}_{q^2}$ and the divisor $rQ_\infty + \sum_{\beta \in K_\alpha} k_\beta P_{\alpha,\beta}$ of H where $\alpha \in \mathbb{F}_{q^2}$, $r \in \mathbb{Z}$, and $k_\beta \in \mathbb{Z}$ for each $\beta \in K_\alpha$. Then*

$$\bigcup_{0 \leq i \leq q} \left\{ (x-\alpha)^i \prod_{\beta \in K_\alpha} \tau_{\alpha,\beta}^{e_{\beta,i}} : -\sum_{\beta \in K_\alpha} \left\lfloor \frac{k_\beta + i}{q+1} \right\rfloor \leq \sum_{\beta \in K_\alpha} e_{\beta,i} \leq \frac{r - iq}{q+1} \right\}$$

is a basis of the space $\mathcal{L}\left(rQ_\infty + \sum_{\beta \in K_\alpha} k_\beta P_{\alpha,\beta}\right)$.

Proof: This follows immediately from Theorem 3.3 and the proof of Theorem 3.6. □

Remark 3.8. We note that Theorem 3.6 may be used to derive the Weierstrass gap set of any m-tuple of consisting of distinct places of the form P_∞ and $P_{\alpha,\beta}$ of a Hermitian function field where $\alpha \in \mathbb{F}_{q^2}$ is fixed. For another approach to determining this Weierstrass gap set, see [11] and [10]. It would also be possible to derive the set of pure gaps of m-tuples of the form $(P_\infty, P_{\alpha,\beta_2}, \ldots, P_{\alpha,\beta_m})$ from Theorem 3.6 for a fixed $\alpha \in \mathbb{F}_{q^2}$.

Theorem 3.9. *Let $G := rQ_\infty + \sum_{\beta\in K_\alpha} k_\beta P_{\alpha,\beta}$ be a divisor of the Hermitian function field $H/\mathbb{F}_{q^2}$ where $r \in \mathbb{Z}$, $\alpha \in \mathbb{F}_{q^2}$, and $k_\beta \in \mathbb{Z}$ for each $\beta \in K_\alpha$. The floor of G is given by*

$$\lfloor G \rfloor = bQ_\infty + \sum_{\beta\in K_\alpha} a_\beta P_{\alpha,\beta}$$

where

$$a_\beta = -\min\left\{ i - (q+1)\left\lfloor \frac{k_\beta + i}{q+1} \right\rfloor : 0 \le i \le q \text{ and } V_i \neq \emptyset \right\},$$

$$b := \max\left\{ (q+1)\left\lfloor \frac{r - iq}{q+1} \right\rfloor + qi : 0 \le i \le q \text{ and } V_i \neq \emptyset \right\},$$

and

$$V_i := \left\{ -(q+1)\sum_{\beta\in K_\alpha} e_\beta - iq : \begin{array}{l} e_\beta \in \mathbb{Z}, -k_\beta \le e_\beta(q+1) + i, \text{ and} \\ (q+1)\sum_{\beta\in K_\alpha} e_{\beta,i} + iq \le r \ \forall \beta \in K_\alpha \end{array} \right\}$$

is as defined in the proof of Theorem 3.6 for $0 \le i \le q$.

Proof: We use Theorem 2.6 and Theorem 3.3. Suppose $V_i \neq \emptyset$. Then from the proof of Theorem 3.6, we have that

$$-\sum_{\beta\in K_\alpha} \left\lfloor \frac{k_\beta + i}{q+1} \right\rfloor \le \left\lfloor \frac{r - iq}{q+1} \right\rfloor,$$

and all elements of V_i are of the form $-(q+1)\sum_{\beta\in K_\alpha} e_\beta - iq$, where $e_\beta \ge -\left\lfloor \frac{k_\beta+i}{q+1} \right\rfloor$ and $\sum_{\beta\in K_\alpha} e_\beta \le \left\lfloor \frac{r-iq}{q+1} \right\rfloor$. Put

$$z = (x-\alpha)^i \prod_{\beta\in K_\alpha} \tau_{\alpha,\beta}^{e_\beta}.$$

Now, we have that the divisor of z is

$$\begin{aligned} (z) &= \sum_{\beta\in K_\alpha} (i + e_\beta(q+1))\, P_{\alpha,\beta} - \left((q+1)\sum_{\beta\in K_\alpha} e_\beta + iq \right) Q_\infty \\ &\ge \sum_{\beta\in K_\alpha} \left(i - (q+1)\left\lfloor \frac{k_\beta + i}{q+1} \right\rfloor \right) P_{\alpha,\beta} - \left((q+1)\left\lfloor \frac{r-iq}{q+1} \right\rfloor + iq \right) Q_\infty. \end{aligned}$$

For each $i, 0 \le i \le q$, let

$$S_i := \left\{ (x-\alpha)^i \prod_{\beta \in K_\alpha} \tau_{\alpha,\beta}^{e_{\beta,i}} : -\sum_{\beta \in K_\alpha} \left\lfloor \frac{k_\beta + i}{q+1} \right\rfloor \le \sum_{\beta \in K_\alpha} e_{\beta,i} \le \frac{r-iq}{q+1} \right\}.$$

By Theorem 3.3 and the proof of Theorem 3.6, $S := \cup_{i=1}^{q} S_i$ is a spanning set of $\mathcal{L}(G)$. By Theorem 2.6,

$$\begin{aligned} \lfloor G \rfloor &= -\gcd((z) : z \in S) \\ &= -\textstyle\sum_{\beta \in K_\alpha} \left(i - (q+1) \left\lfloor \frac{k_\beta + i}{q+1} \right\rfloor \right) P_{\alpha,\beta} + \left((q+1) \left\lfloor \frac{r-iq}{q+1} \right\rfloor + iq \right) Q_\infty \end{aligned}$$

and the desired result follows. □

Example 3.10. Consider the Hermitian function field $F := \mathbb{F}_{64}(x, y)$ where

$$y^8 + y = x^9$$

and ω is a primitive element of $\mathbb{F}_{64}$. Then the genus of F is $g = 28$. According to Theorem 3.9, the floor of

$$H := 12P_\infty + 9P_{0,0} + 10P_{0,1} + 10P_{0,\omega^9}$$

is

$$\lfloor H \rfloor = 9P_\infty + 9P_{0,0} + 9P_{0,1} + 9P_{0,\omega^9}.$$

Set

$$G := H + \lfloor H \rfloor = 21P_\infty + 18P_{0,0} + 19P_{0,1} + 19P_{0,\omega^9}$$

and take D to be the sum of all rational places of F other than those in the support of G. Then $C_\Omega(D, G)$ is a code of length $513 - 4 = 509$ and dimension 459. By Theorem 2.10, the minimum distance of $C_\Omega(D, G)$ is at least 28. There is exactly one one-point code on F (that is, a code of the form $C_\Omega(D + P_{0,0} + P_{0,1} + P_{0,\omega^9}, \alpha P_\infty)$) that has dimension 459. It has length 512, and its minimum distance is exactly 26.

Corollary 3.11. *Let $G := rQ_\infty - \sum_{\beta \in K_\alpha} k_\beta P_{\alpha,\beta}$ be a divisor of the Hermitian function field $H/\mathbb{F}_{q^2}$ where $r \in \mathbb{Z}$, $\alpha \in \mathbb{F}_{q^2}$, and $k_\beta \in \mathbb{Z}$ for each $\beta \in K_\alpha$. Let V_i, $0 \le i \le q$, be as defined in Theorem 3.9. For each $\beta \in K_\alpha$, write $k_\beta = s_\beta(q+1) + m_\beta$ with $0 \le m_\beta \le q$, and write $r = (q+1)r_1 + r_0$ with $0 \le r_0 \le q$. For each $\beta \in K_\alpha$, put $i_\beta := 0$ if $m_\beta = 0$, otherwise put $i_\beta := q + 1 - m_\beta$. Also, if $r_0 = 0$, put $i_r := 0$, otherwise put $i_r = q + 1 - r_0$.*

Then the following are equivalent:

1. *$G = \lfloor G \rfloor$.*
2. *$V_i \ne \emptyset$ for all $i \in \{i_\beta : \beta \in K_\alpha\} \cup \{i_r\}$.*

Thus, if $V_i = \emptyset$ for $i = i_\beta$ (resp. $i = i_r$), then $\mathcal{L}(G) = \mathcal{L}(G - P)$ where $P = P_{\alpha,\beta}$ (resp. $P = Q_\infty$).

PROOF: Put

$$a(i) := i - (q+1)\left\lfloor \frac{k_\beta + i}{q+1} \right\rfloor.$$

Observe that for $0 \leq i \leq q$, the quantity

$$\begin{aligned} a(i) &= i + m_\beta - k_\beta - (q+1)\left\lfloor \frac{i+m_\beta}{q+1} \right\rfloor \\ &= \begin{cases} i + m_\beta - k_\beta & \text{if } i < q+1-m_\beta \\ i + m_\beta - k_\beta - (q+1) & \text{if } i \geq q+1-m_\beta \end{cases} \end{aligned}$$

is strictly increasing for $0 \leq i < q+1-m_\beta$ and also for $q+1-m_\beta \leq i \leq q$ and so achieves a minimum for $i = 0$ or for $i = q+1-m_\beta$. Since $a(0) = m_\beta - k_\beta$ and $a(q+1-m_\beta) = -k_\beta$, it follows that $a(i) \geq -k_\beta$ with equality if and only if $i = q+1-m_\beta$ (if $m_\beta > 0$) or $i = 0$ (if $m_\beta = 0$). Thus $-k_\beta \leq i - (q+1)\left\lfloor \frac{k_\beta+i}{q+1} \right\rfloor$ with equality if and only if $i = i_\beta$. Similarly,

$$-(q+1)\left\lfloor \frac{r-iq}{q+1} \right\rfloor - qi = i + r_0 - r - (q+1)\left\lfloor \frac{i+r_0}{q+1} \right\rfloor \geq -r$$

with equality if and only if $i = i_r$. □

Remark 3.12. Suppose $G := rQ_\infty - \sum_{i=2}^{m} k_i P_{\alpha,\beta_i}$ is an effective divisor of the Hermitian function field $H/\mathbb{F}_{q^2}$ where $\beta_i \neq \beta_j$ for $i \neq j$. Then $G = \lfloor G \rfloor$ if and only if $(r, -k_2, \ldots, -k_m)$ is an element of the Weierstrass semigroup of the m-tuple $(Q_\infty, P_{\alpha,\beta_2}, \ldots, P_{\alpha,\beta_m})$. According to Corollary 3.11, this is the case if and only if $V_i \neq \emptyset$ for all $i \in \{i_\beta : \beta \in K_\alpha\} \cup \{i_r\}$. Therefore,

$$(r, -k_2, \ldots, -k_m) \in H(Q_\infty, P_{\alpha,\beta_2}, \ldots, P_{\alpha,\beta_m})$$

if and only if

$$V_i \neq \emptyset \text{ for all } i \in \{i_\beta : \beta \in K_\alpha\} \cup \{i_r\}.$$

Moreover, Corollary 3.11 implies that $(r, -k_2, \ldots, -k_m)$ is a pure gap of the m-tuple $(Q_\infty, P_{\alpha,\beta_2}, \ldots, P_{\alpha,\beta_m})$ if and only if $V_i = \emptyset$ for all $i \in \{i_\beta : \beta \in K_\alpha\} \cup \{i_r\}$.

4. Applications to construction of low-discrepancy sequences

The results of Section 3 can be applied in a fast implementation of a special method to produce low-discrepancy (that is, very well-distributed) sequences of points in high-dimensional unit cubes. Such

points can then be used in quasi-Monte Carlo methods, e.g. for high-dimensional numerical integration or optimization. Specifically, we produce Niederreiter-Xing sequences ([13], [12], [14] and [16]), which are a subvariety of so-called digital (t, s)-sequences and fulfill the optimal asymptotic order of discrepancy. In the following we give a brief indication of the background of digital (t, s)-sequences.

The general approach to produce such points is the following: to obtain points in the s-dimensional unit cube, choose s infinite matrices over some finite field $\mathbb{F}_b$ and some bijection between $\mathbb{F}_b$ and $dig_b := \{0, \ldots, b-1\}$. Lexicographically order the infinite digit vectors $dig_b^{\mathbb{N}}$. Then for each digit vector we get a point in the unit cube by first taking the bijection to $\mathbb{F}_b^{\mathbb{N}}$, performing the matrix transformation with the resulting vector for each of the s infinite matrices. The s infinite vectors in $\mathbb{F}_b$ are then transformed back into digit vectors by the chosen bijection and interpreted as floating point digits of a real number in $[0, 1)$ for each coordinate, thus giving a point in $[0, 1)^s$. In praxi, we will only require - and in fact can only use - a finite portion of the sequence, say, the first b^m points. This means we can clip the matrices and the vectors to size $m \times m$ and length m. The distribution quality of the resulting point set is closely related to how large sets of linearly independent vectors can be, that consist of inital row vectors from each of these s matrices. (This distribution quality is expressed by a nonnegative integer parameter t, which is the same as in the name "(t, s)-sequence". Basically, the lower t is, the more row vectors can be taken into such a set of independent vectors and the better the resulting point set will be distributed according to the measure of equidistribution called "discrepancy".) The advantage of the Niederreiter-Xing method originates from the fact that it employs as such row vectors the series expansion coefficients of basis vectors of spaces $\mathcal{L}(D)$ of some global function field. Briefly, the requirements are as follows. Let F be a global function field with genus $g(F)$ and $\mathbb{F}_b$ as the full field of constants. Suppose that F has $s+1$ rational places P_∞, P_1, P_2, ..., P_s and let D be a divisor of F of degree $2g(F)$ such that P_∞ is not in the support of D. In order for fast implementation of the method for the construction of low-discrepancy sequences as presented in [14], one requires fast algorithms for the following steps:

1. Compute an explicit basis for the space $\mathcal{L}(D)$.
2. Find explicit bases for each of the spaces $\mathcal{L}(D + jP_i)$ for $1 \leq i \leq s$ and $j = 0, 1, 2, \ldots$.
3. Find expansions of the basis elements above with respect to the place P_∞.

In praxi, again, we will have an assigned m such that we need to perform step 2 only up to $j = m - 1$. Also the expansions in step 3 are only relevant up to m terms. The $s \times m \times m$ coefficients of the expansions are then the entries of the matrices that are used in the setting described above.

Now the connection to Section 3 is given by choosing a Hermitian function field H over $\mathbb{F}_b$ with $b = q^2$ and the following spaces. Using again the notation of Section 1, let $D := 2g(H)Q_\infty = (q^2-q)Q_\infty$ where the Q_∞ is the the common pole of x and y. We also distinguish the place $P_\infty = P_{0,0}$, the common zero of x and y. For the places P_1, ..., P_s, we use any s of the remaining rational places of H. Of course, $s \leq q^3 - 1$. For $\mathcal{L}(D)$, from Proposition 1.1, we can use the basis

$$\{x^i y^j : 0 \leq i, 0 \leq j \leq q-1, \text{ and } (iq + j(q+1)) \leq q^2 - q\}. \tag{16}$$

For the space $\mathcal{L}(D+nP_{\alpha,\beta})$ we use the basis from Corollary 3.4, namely

$$\{\tau_{\alpha,\beta}^{e_i}(x-\alpha)^i : e_i(q+1) + i \geq -n \text{ and } (q+1)e_i + iq \leq q^2 - q\}. \tag{17}$$

Having these bases, it remains to find fast expansions with respect to the place $P_{0,0}$. We use the uniformizer x as the local parameter of $P_{0,0}$. Then one easily shows that

$$y = x^{q+1} + x^{(q+1)q} + x^{(q+1)q^2} + \ldots. \tag{18}$$

Next we need to find expansions of the elements of the set in (17). In particular, one also has to compute the expansion of

$$\tau_{\alpha,\beta}^{-1} = (y - \beta - \alpha^q(x-\alpha))^{-1}$$

for different α and β. But, while α and β vary, the *form* of $\tau_{\alpha,\beta}^{-1}$ remains the same. So, one need only expand the formal expression $(y - \nu - a^q(x-\mu))^{-1}$ *once* and the expansions of *all* remaining $\tau_{\alpha,\beta}^{-1}$ are obtained by mere substitution of μ and ν by α and β respectively. Now the remaining expansions of the set in (17) of the bases elements reduce to polynomial multiplication. We did an implementation of the above procedure using KASH [6]. Below we indicate the different times it took to obtain the points. All computations were done on a 500GHz PC.

$q = 4$**:**	t is at most $g(H)$=6, base $b = q^2 = 16$, number of dimensions $s \leq 63$
For $s = 63$:	
$m = 100$:	time = 4 minutes 20 seconds
$m = 50$:	time = 1 minute 30 seconds
$m = 30$:	time = 44 seconds
$m = 10$:	time = 14 seconds
$q = 8$**:**	t is at most $g(H) = 28$, base $b = q^2 = 64$, number of dimensions $s \leq 510$
For $s = 365$:	
$m = 30$:	time = 16 minutes (here there are about $64^{30} = 2^{180} > 10^{45}$ points)
$m = 50$:	time = 28 minutes

In general for a fixed m the time per dimension was found to be a constant (i.e. time/s). So for $q = 8$ and $m = 30$, it takes about $100 \cdot \frac{16}{365}$ minutes, i.e. about 4 minutes 20 seconds.

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

[4] C. Carvalho and F. Torres, On Goppa codes and Weierstrass gaps at several points, in press.

[5] 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.

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

[7] 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.

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

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

[10] G. L. Matthews, The Weierstrass semigroup of an m-tuple of collinear points on a Hermitian curve, in press.

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

[12] H. Niederreiter, Factorisation of polynomials and some linear algebra problems over finite fields, Linear Algebra Appl. **192** (1993), 301-328.

[13] H. Niederreiter, Psuedorandom numbers and quasirandom points, Z. Agnew. Math. Mech. 73 (1993), T648-T652.

[14] H. Niederreiter and C. Xing , Low discrepancy sequences and global function fields with many rational places, Finite Fields Appl. **2** (1996), no. 3, 241–273.
[15] H. Stichtenoth, Algebraic Function Fields and Codes, Springer, Berlin, 1993.
[16] C. Xing and H. Niederreiter, A construction of low-discrepancy sequences using global function fields, Acta. Arith. **72** (1995), 281-298.