12-2011

Bases and applications of Riemann-Roch Spaces of Function Fields with Many Rational Places

Justin Peachey
Clemson University, jpeache@clemson.edu

Bases and applications of Riemann-Roch spaces of function fields with many rational places

---

A Dissertation
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Doctor of Philosophy
Mathematical Sciences

---

by
Justin D. Peachey
December 2011

Accepted by:
Dr. Gretchen L. Matthews, Committee Chair
Dr. Shuhong Gao
Dr. Hiren Maharaj
Dr. Hui Xue

Table of Contents

Chapter 1

Introduction

Algebraic geometry codes are generalizations of Reed-Solomon codes, which are implemented in nearly all digital communication devices. First described by V.D. Goppa [15, 16] in the 1970s, these codes arise from algebraic curves or, equivalently, algebraic function fields. In ground-breaking work, Tsfasman, Vladut, and Zink show [37] the existence of a sequence of algebraic geometry codes that exceed the Gilbert-Varshamov bound, which was previously thought unbeatable. Since then, work has been done on constructing one-point codes arising from certain classes of function fields. More recently, it has been shown that multipoint algebraic geometry codes can outperform comparable one-point algebraic geometry codes [25, 27]. In both cases, it is desirable that these function fields have many rational places allowing for longer codes. The prototypical example of such a function field is the Hermitian function field which is maximal, meaning the number of rational places meets the Hasse-Weil bound.

Algebraic geometry codes from the Hermitian function field are the most widely studied and understood class of algebraic geometry codes beyond Reed-Solomon codes. This is due to the explicit description of the codes. Furthermore, Hermitian codes have several other desirable properties. For example, the dual of a one-point Hermitian code is a one-

point Hermitian code of the same form. For a complete description of these properties see [35]. While Hermitian codes have many useful properties, one drawback is that Hermitian codes are only defined over alphabets of square order. In 2003, Geil [12] produced a new family of function fields which contain the Hermitian function field as a special case. This family, known as the norm-trace function field, has the advantage that codes from it may be defined over alphabets of size q^r where $r \geq 2$. The main topic of this dissertation is function fields arising from linearized polynomials; these are a generalization of Geil's norm-trace function field. We also consider applications of this function field to error-correcting codes and small-bias sets. Additionally, we study certain Riemann-Roch spaces and codes arising from the Suzuki function field.

The Weierstrass semigroup of a place on a function field is an object of classical interest and is tied to the dimension of associated Riemann-Roch spaces. In this dissertation, we derive Weierstrass semigroups of m-tuples of places on function fields defined by linearized polynomials. In addition, we also discuss Weierstrass semigroups from finite graphs. In 2007, Baker and Norine [4] proved an analogue of the Riemann-Roch Theorem for finite connected graphs. This chapter concludes with a brief discussion of background information.

1.1 Outline

This dissertation is organized as follows. Chapter 2 provides bases for Riemann-Roch spaces of function fields associated with linearized polynomials. Chapters 3 and 4 provide applications of these bases to the design of small-bias sets and determination of Weierstrass semigroups of the norm trace function field, respectively. In Chapter 5, an overview of Riemann-Roch theory on a finite graph is presented followed by our work on Weierstrass semigroups of a finite graph. Chapter 6 studies the Suzuki function field and recent joint work on finding bases for Riemann-Roch spaces of this function field.

1.2 Preliminaries

In this section, we discuss the necessary background information on algebraic function fields and algebraic geometry codes. For in-depth coverage of this material, we refer the reader to [35]. Unless noted otherwise, the definitions and results in this section may be found there. We will let $\mathbb{N}$ denote the nonnegative integers, $\mathbb{Z}^+$ denote the positive integers, $\mathbb{Z}$ denote the set of integers, and $\mathbb{F}_q$ denotes the finite field of q elements where q is a power of a prime. For any set S containing a zero element, $S^* := S \setminus \{0\}$ is the set of nonzero elements of S.

1.2.1 Algebraic function fields

Definition 1. An algebraic function field F/K of one variable over K is an extension field F of K such that F is a finite algebraic extension of $K(x)$ for some element $x \in F$ which is transcendental over K.

Henceforth, we shall simply refer to an algebraic function field as a function field, and we will write F/K to mean F/K is a function field.

Example 1. Let $K = \mathbb{F}_{q^2}$, where q is a power of a prime. Let x be transcendental over K. Then, $F = K(x, y)$ where

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

is a function field since y is a root of $T^q + T - x^{q+1} \in K(x)[T]$. This function field is called the Hermitian function field.

Definition 2. A place P of the function field F/K is the maximal ideal of some valuation ring $\mathcal{O}$ of F/K. Let

$$\mathbb{P}_F := \{P : P \text{ is a place of } F/K\}.$$

Example 2. Consider the rational function field F/K. Then, by [35, Theorem I.2.2] all the places of F/K are of the form $P_{p(x)}$ or P_∞ where

$$P_{p(x)} = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], p(x) | f(x), p(x) \nmid g(x) \right\}$$

and

$$P_\infty = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in K[x], deg\ f(x) < deg\ g(x) \right\}.$$

Definition 3. A discrete valuation of F/K is a function $v : F \to \mathbb{Z} \cup \{\infty\}$ with the following properties:

1. $v(x) = \infty$ if and only if $x = 0$.
2. $v(xy) = v(x) + v(y)$ for any $x, y \in F$.
3. $v(x + y) \geq \min\{v(x), v(y)\}$ for any $x, y \in F$.
4. There exists an element $z \in F$ with $v(z) = 1$.
5. $v(a) = 0$ for any $a \in K \setminus \{0\}$.

Let F/K be a function field and $P \in \mathbb{P}_F$. Let t be a prime element for P and $\mathcal{O}_P$ denote the corresponding valuation ring. Then, every $z \in F \setminus \{0\}$ has a unique representation $z = t^n u$ where $u \in \mathcal{O}_P^*$ and $n \in \mathbb{Z}$. Define $v_P(z) := n$ and $v_P(0) := \infty$. Then, v_P is a discrete valuation of F/K.

Definition 4. Let $P \in \mathbb{P}_F$.

1. The residue class field of P is $F_P := \mathcal{O}_P/P$.
2. The degree of the place P is $deg\ P := [F_P : K]$.

3. The residue class map is

$$\begin{aligned} F &\to F_P \cup \{\infty\} \\ f &\mapsto f + P \end{aligned}$$

where $f + P := \infty$ for $f \notin \mathcal{O}_p$.

Definition 5. Let $z \in F$ and $P \in \mathbb{P}_F$. We say that P is a zero of z if and only if $v_P(z) > 0$; P is a pole of z if and only if $v_P(z) < 0$. If $v_P(z) = m > 0$, P is a zero of z of order m; if $v_P(z) = -m < 0$, P is a pole of z of order m.

Definition 6. The divisor group of F/K, denoted by $\mathcal{D}_F$, is the free abelian group which is generated by the places of F/K. The elements of $\mathcal{D}_F$ are called divisors of F/K.

In other words, a divisor is a sum

$$D = \sum_{P \in \mathbb{P}_F} n_P P \text{ with } n_P \in \mathbb{Z}, \text{ and almost all } n_P = 0.$$

Furthermore, the support of the divisor D is defined by

$$supp\ D := \{P \in \mathbb{P}_F : n_P \neq 0\}.$$

Two divisors $D = \sum_{P \in \mathbb{P}_F} n_P P$ and $D' = \sum_{P \in \mathbb{P}_F} n'_P P$ are added coefficientwise, i.e.,

$$D + D' = \sum_{P \in \mathbb{P}_F} (n_P + n'_P) P.$$

For $Q \in \mathbb{P}_F$ and $D = \sum_{P \in \mathbb{P}_F} n_P P$, we define $v_Q(D) := n_Q$. The degree of a divisor is defined as

$$degD := \sum_{P \in \mathbb{P}_F} v_P(D) \deg P.$$

Finally, we define a partial ordering on $\mathcal{D}_F$ by

$$D_1 \leq D_2 \text{ if and only if } v_P(D_1) \leq v_P(D_2) \text{ for all } P \in \mathbb{P}_F.$$

Definition 7. Let $f \in F \setminus \{0\}$ and denote by Z (respectively N) the set of zeros (poles) of f in $\mathbb{P}_F$. Then, the zero divisor of f is

$$(f)_0 = \sum_{P \in Z} v_P(f)P,$$

the pole divisor of f is

$$(f)_\infty = \sum_{P \in N} (-v_P(f))P,$$

and the divisor of f is

$$(f) = (f)_0 - (f)_\infty.$$

Hence,

$$(f) = \sum_{P \in Z} v_P(f)P + \sum_{P \in N} v_P(f)P.$$

Next, we discuss a special set of functions associated to a divisor A. The functions in this set are determined by their zeros and poles and how these relate to the places in the support of A.

Definition 8. For a divisor $A \in \mathcal{D}_F$, let

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

The set $\mathcal{L}(A)$ is sometimes called the Riemann-Roch space of A. This definition has

the following interpretation. If

$$A = \sum_{i=1}^{r} n_i P_i - \sum_{j=1}^{s} m_j Q_j$$

with $n_i, m_j \in \mathbb{Z}^+$, then $\mathcal{L}(A)$ consists the of the zero function together with all elements $f \in F$ such that

1. f has zeros of order $\geq m_j$ at Q_j, for $j = 1, \ldots, s$, and
2. f may have poles only at the places $P_1, \ldots, P_r$, with the pole order at P_i being bounded by n_i.

Lemma 1. *Given F/K and a divisor $A \in \mathcal{D}_F$, $\mathcal{L}(A)$ is a finite-dimensional vector space over K.*

Furthermore, we define $\ell(A) = dim_K \mathcal{L}(A)$.

Definition 9. The genus g of F/K is defined by

$$g := max\{degA - \ell(A) + 1 : A \in \mathcal{D}_F\}.$$

Definition 10. A divisor W on F/K is a canonical divisor if

$$\deg W = 2g - 2 \text{ and } \ell(W) = g.$$

Now, we have the necessary information to give the following theorem.

Theorem 2. *(Riemann-Roch Theorem) Let W be a canonical divisor of a function field F/K of genus g. Then, for any $A \in \mathcal{D}_F$,*

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

Hence, if A is a divisor of F/K of degree $\deg A \geq 2g-1$ where g denotes the genus of F/K, then

$$\ell(A) = degA + 1 - g.$$

1.2.2 Algebraic coding theory

Given a finite field $\mathbb{F}$ and a positive integer k, $\mathbb{F}^k$ denotes the set of vectors of length k with coordinates in $\mathbb{F}_q$. As usual, given $v \in \mathbb{F}^k$ the i^{th} coordinate of v is denoted by v_i. Given a matrix A, Row_iA denotes the i^{th} row of A and Col_jA denotes the j^{th} column of A. Furthermore, we let A_{ij} denote the entry of A in Row_iA and Col_jA.

Definition 11. A linear code C of length n and dimension k over $\mathbb{F}$ is a k-dimensional $\mathbb{F}$-subspace of the vector space $\mathbb{F}^n$.

Elements of C are called codewords.

This thesis only considers linear codes. Thus, we use the word code to mean linear code.

Definition 12. A generator matrix of a code C of length n and dimension k is

$$\begin{bmatrix} -- & c_1 & -- \\ -- & c_2 & -- \\ & \vdots & \\ -- & c_k & -- \end{bmatrix} \in \mathbb{F}^{k \times n}$$

where $\{c_1, \ldots, c_k\}$ is a basis for C.

A parity check matrix for C is a matrix H such that $Hc = 0$ for all $c \in C$.

Given a code of length n and dimension k, its efficiency may be measured by information rate $\frac{k}{n}$. It is important to have a good information rate; however, a good code must

be able to correct errors as well. The minimum distance provides a measure of a code's error-correcting capability.

Definition 13. The minimum distance of a code C is

$$d = \min \{d(c, c') : c, c' \in C, c \neq c'\},$$

where

$$d(c, c') := |\{i : 1 \leq i \leq n, c_i \neq c'_i\}|$$

is the Hamming distance between c and c'.

We sometimes write $d(C)$ to mean the minimum distance of the code C. The weight of a vector $v \in \mathbb{F}^k$ is $wt(v) = \left|\{i : v_i \neq 0\}\right|$. Note that $d(c, c') = wt(c - c')$. Thus,

$$d(C) = \min\{wt(c) : c \in C \setminus \{0\}\}.$$

Definition 14. A linear code over $\mathbb{F}_q$ of length n and dimension k is called an $[n, k]_q$ code. A linear code over $\mathbb{F}_q$ of length n, dimension k, and minimum distance d (resp. at least d) is called an $[n, k, d]_q$ (resp. $[n, k, \geq d]_q$) code.

When the alphabet is clear from context, we sometimes write $[n, k]$ (resp. $[n, k, d]$, $[n, k, \geq d]$) to mean $[n, k]_q$ (resp. $[n, k, d]_q$, $[n, k, \geq d]_q$). If C has minimum distance d, then C can correct any $\lfloor \frac{d-1}{2} \rfloor$ errors. While it is important to have both a good rate and good error-correcting capability, there is a trade off between the two parameters as demonstrated by the following theorem.

Theorem 3 (Singleton Bound)**.** *For an $[n, k, d]$ code C,*

$$k + d \leq n + 1.$$

Definition 15. The canonical inner product on $\mathbb{F}_q^n$ is defined by

$$\langle a, b\rangle := \sum_{i=1}^{n} a_i b_i,$$

where $a, b \in \mathbb{F}_q$.

Definition 16. If $C \subseteq \mathbb{F}_q^n$ is a code, then

$$C^{\perp} := \{u \in \mathbb{F}_q^n | \langle u, c\rangle = 0 \text{ for all } c \in C\}$$

is called the dual of C.

Notice that the dual of an $[n, k]$ code is an $[n, n-k]$ code. A generator matrix for $C^{\perp}$ is a parity check matrix for a code C. We note that it is also possible to construct a parity check matrix for a code given the generator matrix as discussed in the remark below.

Remark 1. Let C be an $[n, k, d]$ code. If

$$\Big[I_k \Big| H\Big]$$

is a generator matrix for C, then

$$\Big[-H^T \Big| I_{n-k}\Big]$$

is a parity check matrix for C.

Let C_{in} be a $[n, k, d]_q$ code and C_{out} be a $[N, K, D]_{q^k}$. Then, Forney [11] produces a new code by concatenation. Specifically, the inner code C_{in} takes an output of C_{out} and encodes it into an n-tuple over $\mathbb{F}_q$. Then, the information is transmitted and decoded into a possible output of C_{out}. Thus, C_{in} transmits each of the N symbols in a codeword of C_{out}. Such a code is known as the concatenation of C_{out}, the outer code, with C_{in}, the inner code, and is denoted by $C_{out} \circ C_{in}$.

Theorem 4. *Given the above construction, $C_{out} \circ C_{in}$ is an $[nN, kK, \geq dD]_q$ code.*

1.2.3 Algebraic geometry codes

Next, we discuss the construction of algebraic geometry codes, which are codes defined using function fields. Throughout this section, let $\mathbb{F}$ be a finite field.

Definition 17. Given divisors G and $D := Q_1 + \cdots + Q_n$ on a function field $F/\mathbb{F}$ with Q_i distinct places of degree one, $Q_i \notin suppG$, for all i, and $deg\ G < n$,

$$C_{\mathcal{L}}(D, G) := \{(f(Q_1), \ldots, f(Q_n)) : f \in \mathcal{L}(G)\} \subseteq \mathbb{F}^n$$

is an algebraic geometry code.

Proposition 5. *Given divisors G and $D := Q_1 + \cdots + Q_n$ on a function field $F/\mathbb{F}$ as in definition 17, the algebraic geometry code $C_{\mathcal{L}}(D, G)$ defined as in definition 17 is of length n, dimension $k = \ell(G)$, and minimum distance $d \geq n - deg\ G$.*

The code $C_{\mathcal{L}}(D, G)$ is sometimes called an m-point code, where $m = |\text{supp } G|$ is the number of places in the support of the divisor G; if $m > 1$, then $C_{\mathcal{L}}(D, G)$ is a multipoint code. The Riemann-Roch space of G not only governs the dimension of the code but also provides a way to construct generator matrices. If $\{f_1, \ldots, f_k\}$ is a basis for $\mathcal{L}(G)$, then a generator matrix for $C_{\mathcal{L}}(D, G)$ is

$$\begin{bmatrix} f_1(Q_1) & f_1(Q_2) & \cdots & f_1(Q_n) \\ f_2(Q_1) & f_2(Q_2) & \cdots & f_2(Q_n) \\ \vdots & \vdots & & \vdots \\ f_k(Q_1) & f_k(Q_2) & \cdots & f_k(Q_n) \end{bmatrix}.$$

We can associate a second code with the divisors D and G.

Definition 18. Let $P \in \mathbb{P}_F$ and t be a local parameter at P. Let $\omega = fdt$ be a Weil differential. Note that f may be written as $f = \sum_i a_i t^i$. We define the residue of ω at P, $res_P(\omega)$, to be a_{-1}.

Definition 19. Let A be a divisor on a function field $F/\mathbb{F}$. Then, $\Omega(A)$ is the set of Weil differentials η such that $(\eta) \geq A$ along with the zero differential.

Then, we have the following definition.

Definition 20. Given divisors G and $D := Q_1 + \cdots + Q_n$ on a function field $F/\mathbb{F}$ with Q_i distinct places of degree one for all i, $Q_i \notin suppG$,

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

is an algebraic geometry code.

Proposition 6. *Given divisors G and $D := Q_1 + \cdots + Q_n$ on a function field $F/\mathbb{F}$ with Q_i distinct places of degree one for all i, $Q_i \notin suppG$, the code $C_\Omega(D, G)$ defined as in definition 20 is of length n, dimension $k \geq n+g-1-\deg G$, and minimum distance $d \geq \deg\ G-(2g-2)$.*

We note that if $2g - 2 < \deg G < n$, then $k = n + g - 1 - \deg G$. We end this section with the following results which provide the relationship between $C_\Omega(D, G)$ and $C_\mathcal{L}(D, G)$.

Proposition 7. *The codes $C_\Omega(D, G)$ and $C_\mathcal{L}(D, G)$ are dual to one other, i.e.,*

$$C_\mathcal{L}(D, G)^\perp = C_\Omega(D, G).$$

Lemma 8. *Let η be a Weil differential such that $v_{P_i}(\eta) = -1$ and $\eta_{P_i}(1) = 1$ for $i = 1, \ldots, n$. Then,*

$$C_\Omega(D, G) = C_\mathcal{L}(D, D - G + (\eta)).$$

Chapter 2

Riemann-Roch spaces of function fields associated with linearized polynomials

Let q be a power of a prime and r be an integer with $r \geq 2$. Consider the function field $F := \mathbb{F}_{q^r}(x, y)/\mathbb{F}_{q^r}$ which has defining equation

$$L(y) = x^u \tag{2.1}$$

where where $L(y) = \sum_{i=0}^{d} a_i y^{q^i}$ is a linearized polynomial with $a_0, a_d \neq 0$ and q^d distinct roots in $\mathbb{F}_{q^r}$, and $u | \frac{q^r-1}{q-1}$. This function field is called the extended norm-trace function field, because if one takes $u = \frac{q^r-1}{q-1}$ and $L(y) = Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(y)$, the defining equation (2.1) is

$$N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(x) = Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(y),$$

meaning the norm of x with respect to the extension $\mathbb{F}_{q^r}/\mathbb{F}_q$ is equal to the trace of y with respect to the extension $\mathbb{F}_{q^r}/\mathbb{F}_q$. As special cases of the extended norm-trace function

field, one may also obtain the Hermitian function field (by taking $r = 2$ and $u = \frac{q^r-1}{q-1}$) and a quotient of the Hermitian function field (by taking $r = 2$). These function fields are important in coding theory. Hermitian codes, while considered to be the prototype for algebraic geometry codes, only exist over $\mathbb{F}_{q^2}$. Codes constructed from the extended norm-trace function field are defined over $\mathbb{F}_{q^r}$ for any $r \geq 2$. Thus a wider range of alphabet sizes is available for the extended norm-trace function fields. In addition, some codes on the extended norm-trace function field can have better parameters than comparable Hermitian codes [28, 31]. The relevance of this function field to coding theory is tied to the abundance of rational places. Both the Hermitian function field and its quotient mentioned above are maximal function fields, meaning that the number of rational places meet the Hasse-Weil bound. The norm-trace function field (and its infinite place), while not maximal, meet the Geil-Matsumoto bound [13]. Certain places are singled out in the construction of algebraic geometry codes, and the Geil-Matsumoto bound takes this into account.

The norm-trace function field was first studied by Geil in [12] where he considered evaluation codes and one-point algebraic geometry codes constructed from this function field. More recently, Munuera, Tizziotti, and Torres [31] examined two-point algebraic geometry codes on this same function field. In this chapter, we provide explicit bases of Riemann-Roch spaces of divisors supported by certain places of degree one on the norm-trace function field. These bases yield generator and parity check matrices for algebraic geometry codes of the form $C_{\mathcal{L}}\left(D, aP_\infty + \sum_{\beta\in\mathcal{B}} a_\beta P_{0\beta}\right)$ on the extended norm-trace function field. This includes one-point codes as well as multipoint codes supported by any of the places P_∞ or $P_{0\beta}$ on the extended norm-trace function field. The results presented here are generalizations of analogous results for the Hermitian function field given by Stichtenoth in [33, Satz 4] (also see [34, Proposition 1]) and Matthews, Maharaj, and Pirsic in [24, Theorem 3.6]. These provide more general codes together with a description as straightforward as their Hermitian counterparts. Moreover, some of these codes have better parameters. The dimensions of

the Riemann-Roch spaces mentioned above allow one to find the associated Weierstrass semigroups and study parameters of associated algebraic geometry codes.

This chapter is organized as follows. Section 2.1 contains relevant background on the extended norm-trace function field. Section 2.2 includes the main results, which is the determination of bases for and dimensions of certain Riemann-Roch spaces associated with the extended norm-trace function field. In Sections 2.3 and 2.4, the results of Section 2.2 are applied to study algebraic geometry codes associated with the extended norm-trace function field.

2.1 Preliminaries on the extended norm-trace function field

Consider the extended norm-trace function field $F := \mathbb{F}_{q^r}(x, y)/\mathbb{F}_{q^r}$ which has defining equation

$$L(y) = x^u$$

where $L(y) = \sum_{i=0}^{d} a_i y^{q^i}$ is a linearized polynomial with $a_0, a_d \neq 0$ and q^d distinct roots in $\mathbb{F}_{q^r}$, $u | \frac{q^r-1}{q-1}$, q is a power of a prime, and $r \geq 2$ is an integer. Let

$$\mathcal{B} := \{\beta \in \mathbb{F}_{q^r} : L(\beta) = 0\}.$$

Then

$$|\mathcal{B}| = q^d,$$

and for any $\beta \in \mathcal{B}$,

$$L(y - \beta) = x^u.$$

Furthermore, one can show

$$(x) = \sum_{\beta \in \mathcal{B}} P_{0\beta} - q^d P_\infty,$$

and

$$(y - \beta) = uP_{0\beta} - uP_\infty.$$

We view F as a Kummer extension of $\mathbb{F}_{q^r}(y - \beta)$ where $\beta \in \mathcal{B}$. One may notice that the place P_γ of function field $\mathbb{F}_{q^r}(y - \beta)$ corresponds to the irreducible polynomial $(y - \beta) - \gamma = y - (\beta + \gamma)$. If $\gamma \in \mathcal{B}$, then the place P_γ is totally ramified in $F/\mathbb{F}_{q^r}$. The infinite place p_∞ of $\mathbb{F}_{q^r}(y - \beta)$ is also totally ramified in the extension $F/\mathbb{F}_{q^r}$. The genus of $F/\mathbb{F}_{q^r}$ is $g = \frac{(u-1)\left(q^d-1\right)}{2}$.

This class of function fields contains many important families of function fields, including:

- the quotient of a norm-trace function field which has defining equation

$$y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y = x^u.$$

- the norm-trace function field which has defining equation

$$y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y = x^{\frac{q^r-1}{q-1}}.$$

- the quotient of a Hermitian function field which has defining equation

$$y^q + y = x^u,$$

where $u|(q + 1)$.

- the Hermitian function field which has defining equation

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

2.2 Bases for Riemann-Roch spaces on function fields from linearized polynomials

In this section, we determine bases for Riemann-Roch spaces $\mathcal{L}(a_\infty P_\infty + \sum_{\beta\in\mathcal{B}} a_\beta P_{0\beta})$ on the family of function fields arising from certain linearized polynomials. This method is similar to [24].

Lemma 9. *The functions* $1, x, x^2, \ldots, x^{u-1}$ *form an integral basis of the norm-trace function field* $\mathbb{F}_{q^r}(y-\beta, x)/\mathbb{F}_{q^r}(y-\beta)$ *at any place* P_γ*, where* $\beta, \gamma \in \mathcal{B}$*, of* $\mathbb{F}_{q^r}(y-\beta)$*.*

Proof. Let $\beta, \gamma \in \mathcal{B}$. The minimum polynomial of x over $\mathbb{F}_{q^r}(y-\beta)$ is

$$\Phi(T) = T^u - L(y-\beta)$$

according to [35, Theorem III.7.3(a)]. Since P_γ is totally ramified in the extension $F/\mathbb{F}_{q^r}(y-\beta)$ and $q \nmid u$, the different exponent of $P_{0\gamma}$ over P_γ is $d(P_{0\gamma}|P_\gamma) = u-1$. Now, by [35, Theorem III.5.10(b)], we must show that $d(P_{0\gamma}|P_\gamma) = v_{P_{0\gamma}}(\Phi'(x))$ where Φ' denotes the derivative of Φ. Note that

$$v_{P_{0\gamma}}(\Phi'(x)) = v_{P_{0\gamma}}(ux^{u-1}) = (u-1)\, v_{P_{0\gamma}}(x) = u-1$$

since the divisor of the function x is

$$(x) = \sum_{b\in\mathcal{B}} P_{0b} - q^d P_\infty.$$

It now follows that $\{1, x, x^2, \ldots, x^{u-1}\}$ is an integral basis at any place P_γ of $\mathbb{F}_{q^r}(y-\beta)$ with $\gamma \in \mathcal{B}$. $\square$

Theorem 10. *Consider the divisor $G := a_\infty P_\infty + \sum_{\beta\in\mathcal{B}} a_\beta P_{0\beta}$ on the extended norm-trace function field $F/\mathbb{F}_{q^r}$, where $a_\infty \in \mathbb{Z}$ and $a_\beta \in \mathbb{Z}$ for all $\beta \in \mathcal{B}$. Then*

$$\bigcup_{0\le i\le u-1} \left\{ x^i \prod_{\beta\in\mathcal{B}} (y-\beta)^{e_{\beta,i}} : -\sum_{\beta\in\mathcal{B}} \left\lfloor \frac{a_\beta + i}{u} \right\rfloor \le \sum_{\beta\in\mathcal{B}} e_{\beta,i} \le \frac{a_\infty - iq^d}{u} \right\}$$

is a basis for $\mathcal{L}(G)$ as a vector space over $\mathbb{F}_{q^r}$.

Furthermore, the dimension of $\mathcal{L}(G)$ is

$$\ell(G) = \sum_{i=0}^{u-1} \max\left\{ \left\lfloor \frac{a_\infty - iq^d}{u} \right\rfloor + \sum_{\beta\in\mathcal{B}} \left\lfloor \frac{a_\beta + i}{u} \right\rfloor + 1, 0 \right\}.$$

Proof. Let $\mathcal{L} := \mathcal{L}(a_\infty P_\infty + \sum_{\beta\in\mathcal{B}} a_\beta P_{0\beta})$ and

$$S := \left\{ x^i \prod_{\beta\in\mathcal{B}} (y-\beta)^{e_{\beta,i}} : \begin{array}{r} e_{\beta,i} \in \mathbb{Z},\ -a_\beta \le u e_{\beta,i} + i, \\ iq^d + u\sum_{\beta\in\mathcal{B}} e_{\beta,i} \le a_\infty \\ \text{for all } \ i,\ 0 \le i \le u-1 \end{array} \right\}.$$

First, we show that $S \subseteq \mathcal{L}$. Given $0 \le i \le u-1$, the divisor of the function $x^i \prod_{\beta\in\mathcal{B}} (y-\beta)^{e_{\beta,i}}$ is

$$\left(x^i \prod_{\beta\in\mathcal{B}} (y-\beta)^{e_{\beta,i}} \right) = \sum_{\beta\in\mathcal{B}} (u e_{\beta,i} + i) P_{0\beta} - \left(iq^d + u\sum_{\beta\in\mathcal{B}} e_{\beta,i} \right) P_\infty.$$

Since $-a_\beta \le u e_{\beta,i} + i$ and $iq^d + u\sum_{\beta\in\mathcal{B}} e_{\beta,i} \le a_\infty$, $S \subseteq \mathcal{L}$. Hence, the $\mathbb{F}_{q^r}$-linear span of S is a subset of $\mathcal{L}$.

Next, we show that every element of $\mathcal{L}$ can be expressed as a linear combination of elements from S with coefficients from $\mathbb{F}_{q^r}$. Fix $\beta \in \mathcal{B}$, and let $f \in \mathcal{L} \setminus \{0\}$. Then

the only possible poles of f are P_∞ and $P_{0\gamma}$ where $\gamma \in \mathcal{B}$. Thus, by Lemma 9 there exist $f_i \in \mathbb{F}_{q^r}(y-\beta)$ such that

$$f = f_0 + f_1 x + \cdots + f_{u-1} x^{u-1}$$

where the only poles in $\mathbb{F}_{q^r}(y-\beta)$ of the f_i are p_∞ and P_γ where $\gamma \in B$. It follows that

$$f_i = g_i \prod_{\gamma \in \mathcal{B}} (y-\gamma)^{e_{\gamma,i}},$$

where $e_{\gamma,i} \in \mathbb{Z}$, $g_i \in \mathbb{F}_{q^r}[y-\beta]$, and $(y-\gamma) \nmid g_i(y-\beta)$ for all $\gamma \in \mathcal{B}$. Thus, f_i is an $\mathbb{F}_{q^r}$-linear combination of functions

$$A_{i,l} := (y-\beta)^l \prod_{\gamma \in \mathcal{B}} (y-\gamma)^{e_{\gamma,i}}$$

for $l = 0, 1, \ldots, \deg g_i$. Consequently, to prove that f is an $\mathbb{F}_{q^r}$-linear combination of elements of S, it suffices to prove that

$$x^i A_{i,l} \in S$$

for $0 \le i \le u-1$ and $l = 0, 1, \ldots, \deg g_i$. To this end, we note that

$$x^i A_{i,l} = x^i (y-\beta)^{e_{\beta,i}+l} \prod_{\gamma \in \mathcal{B} \setminus \{\beta\}} (y-\gamma)^{e_{\gamma,i}}.$$

Hence, we must show that if $0 \le i \le u-1$ and $l = 0, 1, \ldots, \deg g_i$, then

$$-a_\beta \le u(e_{\beta,i} + l) + i, \tag{2.2}$$

$$-a_\gamma \le u e_{\gamma,i} + i \text{ for } \gamma \in \mathcal{B} \setminus \{\beta\}, \tag{2.3}$$

and

$$iq^d + u\left(l + \sum_{\gamma \in \mathcal{B}} e_{\gamma,i}\right) \leq a_\infty. \tag{2.4}$$

Let $\delta \in \mathcal{B}$. Since $P_{0\delta}$ is totally ramified in the extension $F/\mathbb{F}_{q^r}(y-\beta)$,

$$\begin{aligned} v_{P_{0\delta}}(f_i x^i) &= v_{P_{0\delta}}(f_i) + v_{P_{0\delta}}(x^i) \\ &= uv_{P_\delta}(f_i) + i. \end{aligned}$$

Thus, it is immediate that for $0 \leq i, j \leq u-1$,

$$v_{P_{0\delta}}\left(f_i x^i\right) \not\equiv v_{P_{0\delta}}\left(f_j x^j\right) \mod u$$

unless $i = j$. It follows that

$$v_{P_{0\delta}}(f) = \min\{uv_{P_\delta}(f_i) + i : 0 \leq i \leq u-1\}.$$

This implies

$$uv_{P_\delta}(f_i) + i \geq -a_\delta,$$

because $f \in \mathcal{L}$. Recalling that $f_i = g_i \prod_{\gamma \in \mathcal{B}} (y-\gamma)^{e_{\gamma,i}}$ and $(y-\delta) \nmid g_i$, we see that

$$v_{P_\delta}(f_i) = e_{\delta,i}.$$

Consequently, for $0 \leq i \leq u-1$,

$$-a_\delta \leq ue_{\gamma,i} + i$$

which proves Equation (2.3). Taking $\delta = \beta$ gives

$$-a_\beta \leq ue_{\beta,i} + i \leq u(e_{\beta,i} + l) + i$$

since $0 \leq l$. Hence, Equation (2.2) holds.

It remains to prove Equation (2.4). With this as a goal, note that

$$v_{P_\infty}\left(f_i x^i\right) = v_{P_\infty}\left(f_i\right) + v_{P_\infty}\left(x^i\right) = u v_{p_\infty}\left(f_i\right) - iq^d.$$

Suppose that $u v_{p_\infty}\left(f_i\right) - iq^d \equiv u v_{p_\infty}\left(f_j\right) - jq^d \mod u$ for some j, $0 \leq j \leq u-1$. Then $u|\left(j-i\right)$ since $\gcd(u, q^d) = 1$. However, $|j-i| \leq u-1$ and so $j = i$. Thus,

$$u v_{p_\infty}\left(f_i\right) - iq^d, 0 \leq i \leq u-1$$

are distinct modulo u. Hence,

$$v_{P_\infty}\left(f\right) = \min\{u v_{p_\infty}\left(f_i\right) - iq^d : 0 \leq i \leq u-1\}.$$

Since $f \in \mathcal{L}$,

$$\min\{u v_{p_\infty}\left(f_i\right) - iq^d : 0 \leq i \leq u-1\} \geq -a_\infty.$$

Furthermore, $v_{p_\infty}\left(f_i\right) = -\left(\deg\, g_i + \sum_{\gamma \in \mathcal{B}} e_{\gamma,i}\right)$. Therefore,

$$u\left(\deg g_i + \sum_{\gamma \in \mathcal{B}} e_{\gamma,i}\right) + iq^d \leq a_\infty,$$

and Equation (2.4) holds as $0 \leq l \leq \deg g_i$.

This gives a spanning set for $\mathcal{L}$. Next, we determine the dimension of the Riemann-Roch space $\mathcal{L}(a_\infty P_\infty + \sum_{\beta \in \mathcal{B}} a_\beta P_{0\beta})$ to show the spanning set gives a basis.

For $0 \leq i \leq u-1$ set

$$V_i := \left\{ -iq^d - u\sum_{\beta\in\mathcal{B}} e_\beta : \begin{array}{c} e_\beta \in \mathbb{Z}, -a_\beta \leq ue_\beta + i, \text{ and} \\ iq^d + u\sum_{\beta\in\mathcal{B}} e_\beta \leq a_\infty \\ \text{for all } \beta \in B \end{array} \right\}$$

and

$$V := \cup_{i=0}^{u-1} V_i.$$

We claim that

$$V = \{v_{P_\infty}(f) : f \in \mathcal{L} \setminus \{0\}\}.$$

Let $f \in \mathcal{L} \setminus \{0\}$. It follows from above that $v_{P_\infty}(f) \in V_i$ for some i. Hence,

$$\{v_{P_\infty}(f) : f \in \mathcal{L} \setminus \{0\}\} \subseteq V.$$

To prove the claim, it remains to show that $V \subseteq \{v_{P_\infty}(f) : f \in \mathcal{L} \setminus \{0\}\}$.

Let $n \in V$. Then $n \in V_i$ for some i, $0 \leq i \leq u-1$, and there exists $\{e_\beta : \beta \in \mathcal{B}\}$ so that

$$n = -iq^d - u\sum_{\beta\in\mathcal{B}} e_\beta,$$

$$-a_\beta \leq ue_\beta + i,$$

and

$$iq^d + u\sum_{\beta\in\mathcal{B}} e_\beta \leq a_\infty.$$

Then $v_{P_\infty}\left(x^i \prod_{\beta\in\mathcal{B}} (y-\beta)^{e_\beta}\right) = n$, and $x^i \prod_{\beta\in\mathcal{B}} (y-\beta)^{e_\beta} \in \mathcal{L}$ by previous argument. Hence, $V = \{v_{P_\infty}(f) : f \in \mathcal{L} \setminus \{0\}\}$, and the claim holds. Moreover, by [24, Lemma

3.5],

$$\dim \mathcal{L} = |V|.$$

Consequently, we next find $|V|$.

To do so, we claim that the sets V_i, $0 \leq i \leq u-1$, are disjoint. Suppose $n \in V_i \cap V_j$ for some $0 \leq i, j \leq u-1$. Then $u | (i-j) q^d$. As shown above, it follows that $i = j$. This establishes the claim that the sets V_i, $0 \leq i \leq u-1$, are disjoint. Therefore,

$$\dim \mathcal{L} = |V| = \sum_{i=0}^{u-1} |V_i|.$$

It remains to determine $|V_i|$.

Fix i, $0 \leq i \leq u-1$, and set $n := -iq^d - cu$ where $c \in \mathbb{Z}$. Then $n \in V$ if and only if $n \in V_i$; that is, $n \in V$ if and only if

$$-iq^d - cu = -iq^d - u \sum_{\beta \in \mathcal{B}} e_\beta$$

for some $e_\beta \in \mathbb{Z}$ with

$$-a_\beta \leq e_\beta u + i$$

and

$$iq^d + u \sum_{\beta \in \mathcal{B}} e_\beta \leq a_\infty.$$

Hence, $n \in V$ if and only if there exist e_β for $\beta \in \mathcal{B}$ so that

$$c = \sum_{\beta \in \mathcal{B}} e_\beta$$

and

$$\sum_{\beta \in \mathcal{B}} e_\beta \leq \frac{a_\infty - iq^d}{u}.$$

Further, note that $e_\beta \geq \left\lceil -\frac{a_\beta+i}{u} \right\rceil = -\left\lfloor \frac{a_\beta+i}{u} \right\rfloor$. Thus, such e_β exist if and only if

$$-\sum_{\beta\in\mathcal{B}} \left\lfloor \frac{a_\beta+i}{u} \right\rfloor \leq c = \sum_{\beta\in\mathcal{B}} e_\beta \leq \frac{a_\infty - iq^d}{u}.$$

We conclude that $-iq^d - cu \in V_i$ if and only if

$$-\sum_{\beta\in\mathcal{B}} \left\lfloor \frac{a_\beta+i}{u} \right\rfloor \leq c \leq \frac{a_\infty - iq^d}{u}.$$

It follows that

$$|V_i| = \left| \mathbb{Z} \cap \left[-\sum_{\beta\in\mathcal{B}} \left\lfloor \frac{a_\beta+i}{u} \right\rfloor, \frac{a_\infty - iq^d}{u} \right] \right|.$$

Hence,

$$|V_i| = \max\left\{ \left\lfloor \frac{a_\infty - iq^d}{u} \right\rfloor + \sum_{\beta\in\mathcal{B}} \left\lfloor \frac{a_\beta+i}{u} \right\rfloor + 1, 0 \right\}.$$

Therefore,

$$\dim\, \mathcal{L} = |V| = \sum_{i=0}^{u-1} |V_i|\,.$$

Thus, the dimension of $\mathcal{L}\,(G)$ is

$$\ell\,(G) = \sum_{i=0}^{u-1} \max\left\{ \left\lfloor \frac{a_\infty - iq^d}{u} \right\rfloor + \sum_{\beta\in\mathcal{B}} \left\lfloor \frac{a_\beta+i}{u} \right\rfloor + 1, 0 \right\}.$$

Furthermore, note that since S spans $\mathcal{L}(G)$ and $|S| = \ell(G)$,

$$\bigcup_{0\leq i\leq u-1} \left\{ x^i \prod_{\beta\in\mathcal{B}} (y-\beta)^{e_{\beta,i}} : -\sum_{\beta\in\mathcal{B}} \left\lfloor \frac{a_\beta+i}{u} \right\rfloor \leq \sum_{\beta\in\mathcal{B}} e_{\beta,i} \leq \frac{a_\infty - iq^d}{u} \right\}$$

is a basis for $\mathcal{L}(G)$. $\square$

By setting $r = 2$ and $u = q+1$, one recovers bases for Riemann-Roch spaces of the Hermitian function field [24, Corollary 3.7]. In particular, setting $a_\beta = 0$ for all $\beta \in \mathcal{B}$ yields

the original result of Stichtenoth [33, Satz 2] (see also [34, Proposition 1]).

As a consequence of Theorem 10, the floors of divisors with support among the places P_∞ and $P_{0\beta}$, $\beta \in \mathcal{B}$, on the extended norm-trace function field may computed using the lemma below. The floor of a divisor is introduced by Matthews, Maharaj, and Pirsic in [24].

Definition 21. Let G be a divisor on a function field $F/\mathbb{F}$ with $\mathcal{L}(G) \neq \{0\}$. The floor of G, denoted $\lfloor G \rfloor$ is the divisor on $F/\mathbb{F}$ of minimum degree such that

$$\mathcal{L}(G) = \mathcal{L}(\lfloor G \rfloor).$$

Lemma 11. *[24, Theorem 2.6] Let G be a divisor on a function field $F/\mathbb{F}$ with $\mathcal{L}(G) \neq \{0\}$. If $f_1, \ldots, f_k$ form a spanning set for $\mathcal{L}(G)$, then the floor of G is*

$$\lfloor G \rfloor = -\gcd\{(f_i) : 1 \leq i \leq k\}.$$

Thus, we have the following lemma.

Lemma 12. *The floor of $G = a_1 P_\infty + a_2 P_{0\beta_2} + \cdots + a_m P_{0\beta_m}$ on the extended norm-trace function field over $\mathbb{F}_{q^r}$ is*

$$\begin{aligned} \lfloor G \rfloor &= \max\left\{ iq^d + u\left\lfloor \tfrac{a_1 - iq^d}{u} \right\rfloor : \begin{array}{l} 0 \leq i \leq u-1, \\ \left\lfloor \frac{a_1 - iq^{r-1}}{u} \right\rfloor + \sum_{j=2}^m \left\lfloor \frac{a_j + i}{u} \right\rfloor \geq 0 \end{array} \right\} P_\infty \\ &\quad + \sum_{j=2}^m \max\left\{ u\left\lfloor \tfrac{a_j + i}{u} \right\rfloor - i : \begin{array}{l} 0 \leq i \leq u-1, \\ \left\lfloor \frac{a_1 - iq^d}{u} \right\rfloor + \sum_{j=2}^m \left\lfloor \frac{a_j + i}{u} \right\rfloor \geq 0 \end{array} \right\} P_{0\beta_j} \end{aligned}$$

provided $\mathcal{L}(G) \neq \{0\}$.

2.3 Algebraic geometry codes on function fields from linearized polynomials

We begin this section with a brief review of algebraic geometry (AG) codes; for a more thorough discussion, see [20, 35]. Consider an algebraic function field $F/\mathbb{F}$ where $\mathbb{F}$ is a finite field. Let G be a divisor of $F/\mathbb{F}$ and let $D = P_1 + \cdots + P_n$ be another divisor of F where $P_1, \ldots, P_n$ are distinct places of degree one, each not belonging to the support of G. Recall that the AG code $C_{\mathcal{L}}(D, G)$ is

$$C_{\mathcal{L}}(D, G) := \{(f(P_1), f(P_2), \ldots, f(P_n)) : f \in L(G)\}.$$

Recall that such a code $C_{\mathcal{L}}(D, G)$ is sometimes called an m-point code where $m = |SuppG|$. If $\deg G < n$, then the code $C_{\mathcal{L}}(D, G)$ has length n, dimension $\ell(G) \geq \deg G + 1 - g$, and minimum distance at least $n - \deg G$. There are various methods for improving the bound on the minimum distance of an AG code (see [9] for a discussion). Among these, the most intuitive may be the floor bound [24] which notes that the minimum distance of a nonzero AG code $C_{\mathcal{L}}(D, G)$ is at least $n - \deg \lfloor G \rfloor$; this is due to the fact that $\mathcal{L}(G) = \mathcal{L}(\lfloor G \rfloor)$ which implies

$$C_{\mathcal{L}}(D, G) = C_{\mathcal{L}}(D, \lfloor G \rfloor).$$

Theorem 13. *Let $G = a_1 P_\infty + a_2 P_{0\beta_2} + \cdots + a_m P_{0\beta_m}$ and $D = P_1 + \cdots + P_n$ be divisors on the extended norm-trace function field over $\mathbb{F}_{q^r}$ where D is the sum of all places of degree one other than those in the support of G. Then $C_{\mathcal{L}}(D, G)$ has length n, dimension*

$$\sum_{i=0}^{u-1} \max\left\{ \left\lfloor \frac{a_1 - iq^d}{u} \right\rfloor + \sum_{i=2}^{m} \left\lfloor \frac{a_i + i}{u} \right\rfloor + 1, 0 \right\},$$

and minimum distance at least

$$n - \left(\begin{array}{l} \max \left\{ iq^d + u \left\lfloor \frac{a_1 - iq^d}{u} \right\rfloor : \begin{array}{l} 0 \leq i \leq u-1, \\ \left\lfloor \frac{a_1 - iq^d}{u} \right\rfloor \geq -\sum_{j=2}^{m} \left\lfloor \frac{a_j + i}{u} \right\rfloor \end{array} \right\} \\ \\ + \sum_{j=2}^{m} \max \left\{ u \left\lfloor \frac{a_j + i}{u} \right\rfloor - i : \begin{array}{l} 0 \leq i \leq u-1, \\ \left\lfloor \frac{a_1 - iq^d}{u} \right\rfloor \geq -\sum_{j=2}^{m} \left\lfloor \frac{a_j + i}{u} \right\rfloor \end{array} \right\} \end{array} \right).$$

Proof. The dimension of $C_{\mathcal{L}}(D, G)$ follows from Theorem 10, and the bound on the minimum distance can be found by applying Theorem 12. □

In the case of the quotient of a norm-trace function field, we can say more. Specifically, there are exactly $q^{r-1} + u(q^r - q^{r-1}) + 1$ places of degree one in the extended norm-trace function field: a place $P_{\alpha\gamma}$ for every pair of $\alpha, \gamma \in \mathbb{F}_{q^r}$ with $\alpha^u = Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\gamma)$ and P_∞. The structure of this function field also allows us to obtain further results on the parameters of certain algebraic geometry codes.

Corollary 14. *Let $G = a_1 P_\infty + a_2 P_{0\beta_2} + \cdots + a_m P_{0\beta_m}$ and $D = P_1 + \cdots + P_n$ be divisors on the quotient of a norm-trace function field over $\mathbb{F}_{q^r}$ where D is the sum of all places of degree one other than those in the support of G. Then $C_{\mathcal{L}}(D, G)$ has length $n = q^{r-1} + u(q^r - q^{r-1}) + 1$, dimension*

$$\sum_{i=0}^{u-1} \max \left\{ \left\lfloor \frac{a_1 - iq^{r-1}}{u} \right\rfloor + \sum_{i=2}^{m} \left\lfloor \frac{a_i + i}{u} \right\rfloor + 1, 0 \right\},$$

and minimum distance at least

$$n - \left(\begin{array}{l} \max \left\{ iq^{r-1} + u \left\lfloor \frac{a_1 - iq^{r-1}}{u} \right\rfloor : \begin{array}{l} 0 \leq i \leq u-1, \\ \left\lfloor \frac{a_1 - iq^{r-1}}{u} \right\rfloor \geq -\sum_{j=2}^{m} \left\lfloor \frac{a_j + i}{u} \right\rfloor \end{array} \right\} \\ \\ + \sum_{j=2}^{m} \max \left\{ u \left\lfloor \frac{a_j + i}{u} \right\rfloor - i : \begin{array}{l} 0 \leq i \leq u-1, \\ \left\lfloor \frac{a_1 - iq^{r-1}}{u} \right\rfloor \geq -\sum_{j=2}^{m} \left\lfloor \frac{a_j + i}{u} \right\rfloor \end{array} \right\} \end{array} \right).$$

The dual of an AG code $C_{\mathcal{L}}(P_1 + \cdots + P_n, G)$ is the AG code

$$C_{\Omega}(D, G) := \{(res_{P_1}(\eta), res_{P_2}(\eta), \ldots, res_{P_n}(\eta)) : \eta \in \Omega(G - D)\},$$

where $\Omega(A)$ denotes the set of rational differentials η of $F/\mathbb{F}_q$ with divisor $(\eta) \geq A$ together with the zero differential and $res_P(\eta)$ denotes the residue of η at the place P. However, the next result shows that the dual of a multipoint code $C_{\mathcal{L}}(D, a_1 P_{\infty} + a_2 P_{0b_2} + \cdots + a_m P_{0b_m})$ on the norm-trace function field is again a multipoint code of the same form. This result is similar to those of [6] for certain one-point codes on the norm-trace function field and [36, Theorem 1] for one-point Hermitian codes.

Theorem 15. *Let $G = a_1 P_{\infty} + a_2 P_{0\beta_2} + \cdots + a_m P_{0\beta_m}$ and $D = P_1 + \cdots + P_n$ be divisors on the extended norm-trace function field over $\mathbb{F}_{q^r}$ where D is the sum of all places of degree one other than those in the support of G. Then the dual of $C_{\mathcal{L}}(D, G)$ is*

$$C_{\mathcal{L}}(D, G)^{\perp} = C_{\mathcal{L}}\left(D, (u(q^r - m) - 1 - a_1) P_{\infty} + \sum_{j=2}^{m} (u - a_j - 1) P_{0\beta_j}\right).$$

Proof. This is an immediate consequence of [35, Proposition II.2.10] which yields that

$$C_{\Omega}(D, G) = C_{\mathcal{L}}(D, D - G + (\eta))$$

where $\eta = \frac{dy}{\prod_{\beta \in \mathcal{B} \setminus \{\beta_2, \ldots, \beta_m\}} (y-\beta) \prod_{\alpha \in \mathbb{F}_{q^r}, \alpha^u \in \mathbb{F}_q} x-\alpha}$. $\square$

Given a basis $\{f_1, \ldots, f_k\}$ of $\mathcal{L}(G)$, any matrix whose rows are precisely

$$\left(f_i(P_1), f_i(P_2), \ldots, f_i(P_n)\right), 1 \leq i \leq k,$$

is a generator matrix for $C_{\mathcal{L}}(D, G)$. At times, it is more convenient to have a code described in terms of a parity-check matrix. The next result gives both generator and parity-check matrices for the codes considered above.

Proposition 16. *Let $G = a_1 P_\infty + a_2 P_{0\beta_2} + \cdots + a_m P_{0\beta_m}$ and $D = P_1 + \cdots + P_n$ be divisors on the quotient of a norm-trace function field over $\mathbb{F}_{q^r}$ where D is the sum of all places of degree one other than those in the support of G. A generator matrix for $C_{\mathcal{L}}(D, G)$ may be formed by taking rows*

$$x^i \prod_{j=2}^{m} (y-\beta_j)^{e_{ij}} (P_1), x^i \prod_{j=2}^{m} (y-\beta_j)^{e_{ij}} (P_2), \ldots, x^i \prod_{j=2}^{m} (y-\beta_j)^{e_{ij}} (P_n)$$

where $0 \leq i \leq u-1$ and $-\sum_{j=2}^{m} \left\lfloor \frac{a_j+i}{u} \right\rfloor \leq \sum_{j=2}^{m} e_{ij} \leq \frac{a_1 - iq^{r-1}}{u}$. A parity-check matrix for $C_{\mathcal{L}}(D, G)$ may be formed by taking rows

$$x^i \prod_{j=2}^{m} (y-\beta_j)^{e_{ij}} (P_1), x^i \prod_{j=2}^{m} (y-\beta_j)^{e_{ij}} (P_2), \ldots, x^i \prod_{j=2}^{m} (y-\beta_j)^{e_{ij}} (P_n)$$

where $0 \leq i \leq u-1$ and $-\sum_{j=2}^{m} \left\lfloor \frac{i-a_j-1}{u} \right\rfloor \leq \sum_{j=2}^{m} e_{ij} \leq q^r - m - \frac{a_1+1+iq^{r-1}}{u}$.

Proof. Theorem 10 provides the generator matrix given above. Then, Theorem 10 and Theorem 15 yield the parity check matrix. $\square$

We now can utilize the similar structure of $C_{\mathcal{L}}(D, a_1 P_\infty + a_2 P_{0b_2} + \cdots + a_m P_{0b_m})$ and its dual code to find better bounds on the minimum distance of the code. First, we need the

following result from [10, Theorem 2.4].

Theorem 17. *Let K be a canonical divisor on F/K and $G = K + C = A + B + Z$, for some divisors A, B, and $Z \geq 0$ such that $D \cap Z = \emptyset$. Then,*

$$d(C_\Omega(D, G)) \geq \ell(A) - \ell(A - C) + \ell(B) - \ell(B - C).$$

Now, applying this result we obtain the following bound on the minimum distance for certain codes arising from the quotient of a norm-trace function field.

Theorem 18. *Let $G = a_1 P_\infty + a_2 P_{0\beta_2} + \cdots + a_m P_{0\beta_m}$ and $D = P_1 + \cdots + P_n$ be divisors on the extended norm-trace function field over $\mathbb{F}_{q^r}$ where D is the sum of all places of degree one other than those in the support of G. Then, $C_{\mathcal{L}}(D, G)$ has minimum distance at least*

$$\begin{array}{l}
\sum_{i=0}^{u-1} \max\left\{ \left\lfloor \frac{\alpha_1 - iq^{r-1}}{u} \right\rfloor + \sum_{j=2}^{m} \left\lfloor \frac{\alpha_j + i}{u} \right\rfloor + 1, 0 \right\} - \\
\sum_{i=0}^{u-1} \max\left\{ \left\lfloor \frac{-(\beta_1 + \gamma_1) - iq^{r-1}}{u} \right\rfloor + \sum_{j=2}^{m} \left\lfloor \frac{-(\beta_j + \gamma_j) + i}{u} \right\rfloor + 1, 0 \right\} + \\
\sum_{i=0}^{u-1} \max\left\{ \left\lfloor \frac{\beta_\infty - iq^{r-1}}{u} \right\rfloor + \sum_{j=2}^{m} \left\lfloor \frac{\beta_j + i}{u} \right\rfloor + 1, 0 \right\} - \\
\sum_{i=0}^{u-1} \max\left\{ \left\lfloor \frac{-(\alpha_1 + \gamma_1) - iq^{r-1}}{u} \right\rfloor + \sum_{j=2}^{m} \left\lfloor \frac{-(\alpha_j + \gamma_j) + i}{u} \right\rfloor + 1, 0 \right\}
\end{array}$$

where $\alpha_1 + \beta_1 + \gamma_1 = u(q^r - m) - 1 - a_1$ and $\gamma_1 \geq 0$ and $\alpha_j + \beta_j + \gamma_j = u - a_j - 1$ and $\gamma_j \geq 0$ for $2 \leq j \leq m$.

Proof. This theorem is an immediate consequence of Theorem 10, Theorem 15, and Theorem 17, and the fact that $K = (2g - 2)P_\infty$ is a canonical divisor. □

These results can be extended to other bounds utilizing ideas from [10] such as the ABZ+ bound. This is a topic of future study.

2.4 Examples

In this section, we consider examples of algebraic geometry codes described in the previous section.

Example 3. Let $F := \mathbb{F}_8(x, y)/\mathbb{F}_8$ be the norm-trace function field with defining equation $y^4 + y^2 + y = x^7$. We can show there are 33 $\mathbb{F}_8$-rational places. Thus, a two point code has length $n = 31$. Let $G = 20P_\infty + 8P_{0\beta}$. Then, $C_\Omega(D, G) = C_\mathcal{L}(D, 21P_\infty - 2P_{0\beta})$. We can apply this to find both the generator and parity check matrices as previously mentioned. Furthermore, applying Theorem 10, we find that $\ell(G) = 20$. We may use Theorem 18 to see that $C_\mathcal{L}(D, G)$ is a $[31, 20, \geq 5]$ code.

Example 4. Let $F := \mathbb{F}_{16}(x, y)/\mathbb{F}_{16}$ be a quotient of norm-trace function field with defining equation $y^8+y^4+y^2+y = x^5$. We can show there are 49 $\mathbb{F}_{16}$-rational places. Thus, a two point code has length $n = 47$. Let $G = 19P_\infty + 15P_{0\beta}$. Then, $C_\Omega(D, G) = C_\mathcal{L}(D, 50P_\infty - 9P_{0\beta})$. We can apply this to find both the generator and parity check matrices as previously mentioned. Furthermore, applying Theorem 10, we find that $\ell(G) = 21$. We may use Theorem 18 to see that $C_\mathcal{L}(D, G)$ is a $[47, 21, \geq 14]$ code.

Chapter 3

Small-bias sets from a quotient of norm-trace function field

Consider a binary random variable $X := x_1, \ldots, x_k$. Let Ω denote the associated sample space. As shown by Varizani in 1986 [38], the bits $x_1, \ldots, x_k$ of X are independent and uniformly distributed if and only if for all nonempty $T \subseteq \{1, \ldots, k\}$,

$$Prob\left(\sum_{i \in T} x_i = 0\right) = Prob\left(\sum_{i \in T} x_i = 1\right)$$

where the sums are taken in $\mathbb{F}_2$, the finite field with two elements. Of course, if these equivalent conditions are satisfied, then $\Omega = \mathbb{F}_2^k$, the set of binary vectors of length k.

For a fixed k, it is useful in a number of applications to have a sample space that is smaller than $\mathbb{F}_2^k$ yet retains some of its randomness properties. These applications include derandomization of algorithms, testing of combinatorial circuits, and probabilistically checkable proofs. This need for probability spaces that, in some sense, approximate larger ones prompted the notion of a small-bias set.

Definition 22. A subset $X \subseteq \mathbb{F}_2^k$ is ϵ-biased if and only if for all nonempty $T \subseteq \{1, \ldots, k\}$,

$$\frac{1}{|X|} \left| \sum_{x \in X} (-1)^{\sum_{i \in T} x_i} \right| \leq \epsilon.$$

Example 5. Fix a positive integer k. Then the set $\mathbb{F}_2^k$ is 0-biased. On the other hand, $\{v\}$ is 1-biased for any $v \in \mathbb{F}_2^k$.

Given an ϵ-biased set X, ϵ provides a measure of how far from uniform the distribution associated with X is. To make this precise, let U_k denote the uniform distribution on a variable with k bits, and let

$$\Delta(X, Y) := \frac{1}{2} \sum_{\alpha \in \{0,1\}^k} \Big| Prob\left[X = \alpha\right] - Prob\left[Y = \alpha\right] \Big|$$

be the statistical difference between two k-bit random variables X and Y (equivalently, the statistical difference between their distributions).

Remark 2. Suppose $X \subseteq \mathbb{F}_2^k$ is an ϵ-biased set. Then

$$\epsilon \leq \Delta(X, U_k) \leq \sqrt{2^k}\epsilon.$$

Certainly, a set is 0-biased if and only if the associated random variable is uniformly distributed.

While a random set of size $\mathcal{O}\left(\frac{k}{\epsilon^2}\right)$ is ϵ-biased, there is a need for explicit constructions for small-bias sets. The goal of this chapter is to construct ϵ-biased sets $X \subseteq \mathbb{F}_2^k$ for fixed k and ϵ with $|X|$ small.

Our primary tool in the construction of small-bias sets is error-correcting codes. Thus, this section concludes with terminology and notation from coding theory. Section 3.1 contains a tutorial on the construction of small-bias sets from algebraic geometry codes. This

is followed by Section 3.2 detailing the application of algebraic geometry codes from the quotient of norm-trace function field. The chapter concludes with examples given in Section 3.3.

3.1 Balanced codes and small-bias sets

In this section, we review the explicit construction of small-bias sets from balanced codes.

Definition 23. An ϵ-balanced code is a binary code C of length n such that for all nonzero $c \in C$

$$\frac{1-\epsilon}{2} \leq \frac{wt(c)}{n} \leq \frac{1+\epsilon}{2}.$$

Example 6. Given $s \in \mathbb{Z}^+$, the Walsh-Hadamard code C_s is a $[2^s, s]_2$ code with generator matrix

$$\begin{bmatrix} | & | & & | \\ v_1 & v_2 & \cdots & v_{2^s} \\ | & | & & | \end{bmatrix}$$

where $\mathbb{F}_2^s = \{v_1, \ldots, v_{2^s}\}$. It is well-known that C_s is a constant-weight code, and

$$wt(c) = 2^{s-1}$$

for all codewords $c \in C \setminus \{0\}$.

Thus, the Walsh-Hadamard code is a 0-balanced code.

The relationship between ϵ-balanced codes and ϵ-biased sets may be seen in the following lemma.

Lemma 19. *[32] Suppose C is an $[n, k]_2$ code which is ϵ-balanced for some $0 \leq \epsilon \leq 1$. Let*

M be a generator matrix of C and

$$X = \{Col_1 M, Col_2 M, \ldots, Col_n M\}.$$

Then $X \subseteq \mathbb{F}_2^k$ is an ϵ-biased set with cardinality $|X| = n$.

Proof. Suppose C is an $[n,k]_2$ code which is ϵ-balanced for some $0 \leq \epsilon \leq 1$. Let

$$X = \{Col_1 M, Col_2 M, \ldots, Col_n M\}$$

be the set of columns of a generator matrix M of C. Given nonempty $T \subseteq \{1, \ldots, k\}$, define $v \in \mathbb{F}_2^k$ by $v_i = 1$ if and only if $i \in T$. Then

$$\begin{aligned} \tfrac{1}{|X|} \left| \sum_{x \in X} (-1)^{\sum_{i \in T} x_i} \right| &= \tfrac{1}{n} \left| \sum_{j=1}^{n} (-1)^{vcol_j M} \right| \\ &= \tfrac{1}{n} |n - 2wt(vM)| \\ &\leq \tfrac{1}{n} n\epsilon = \epsilon. \end{aligned}$$

Therefore, X is an ϵ-biased set. $\square$

To obtain ϵ-balanced codes from algebraic geometry codes, we utilize a Walsh-Hadamard code.

Fix an algebraic function field $F/\mathbb{F}_{2^s}$. Consider the AG code $C_{\mathcal{L}}(D, G)$ where G and $D := P_1 + \cdots + P_n$ are divisors on F with $P_i \notin \text{supp } G$ for all i and $deg\ G < n$. Concatenating $C_{\mathcal{L}}(D, G)$ with the Walsh-Hadamard code of length 2^s produces an

$$[n2^s, s\ell(G), \geq 2^{s-1}(n - \deg G)]_2$$

code C which is $\frac{\deg G}{n}$-balanced. Hence, the columns of a generator matrix for C form a $\frac{\deg G}{n}$-biased set $X \subseteq \mathbb{F}_2^{s\ell(G)}$ with $|X| = n2^s$. As a result, we have the following theorem.

Theorem 20. *An algebraic geometry code $C_{\mathcal{L}}(D, G)$ of length n over $\mathbb{F}_{2^s}$, with $\deg G < n$, gives rise to a $\frac{\deg G}{n}$-biased set $X \subseteq \mathbb{F}_2^{s\ell(G)}$ with $|X| = n2^s$.*

Example 7. Consider the code $C_{\mathcal{L}}(D, (k-1)P)$ on the rational function field $\mathbb{F}_q(x)/\mathbb{F}_q$ where $q = 2^s$, $k \in \mathbb{Z}^+$, P is the infinite place of $\mathbb{F}_q(x)$, and D is the sum of all other places of degree one; that is, take $C_{\mathcal{L}}(D, (k-1)P)$ to be the $[2^s, k, 2^s - k + 1]_{2^s}$ Reed-Solomon code. Applying Lemma 20 results in a $\frac{k}{2^s}$-bias set $X \subseteq \mathbb{F}_2^k$ with cardinality $\left|X\right| = 2^{2s}$. This now standard construction first appeared in [1].

In the next section, we apply the construction in Theorem 20 to quotient of norm-trace codes.

3.2 Quotient of norm-trace codes and associated ϵ-biased sets

In this section, we consider a generalization of the Hermitian function field, associated AG codes, and resulting small-bias sets. The quotient of norm-trace function field is studied in [6, 12, 30]. Recall that the quotient of norm-trace function field over $\mathbb{F}_{q^r}$ is $\mathbb{F}_{q^r}(x, y)$ where

$$Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(y) = x^u$$

and $u > 1$ is a divisor of $\frac{q^r-1}{q-1}$.

The quotient of norm-trace function field $F/\mathbb{F}_{q^r}$ has genus $g = \frac{(u-1)\left(q^{r-1}-1\right)}{2}$ and exactly

$$q^{r-1}(uq - u + 1) + 1$$

places of degree one. Moreover, it was shown in Chapter 2 that the dimension of the divisor αP_∞, where $\alpha \in \mathbb{Z}^+$ and P_∞ denotes the infinite place of F is

$$\ell(\alpha P_\infty) = \sum_{i=0}^{u-1} \max\left\{ \left\lfloor \frac{\alpha - iq^{r-1}}{u} \right\rfloor + 1, 0 \right\}. \tag{3.1}$$

Consider the AG code $C_{\mathcal{L}}(D, \alpha P_\infty)$ over the quotient of norm-trace function field, where $D = Q_1 + \cdots + Q_{q^{r-1}(uq-u+1)}$ is the sum of all places of degree one other than P_∞ and

$$\alpha < q^{r-1}(uq - u + 1).$$

Then $C_{\mathcal{L}}(D, \alpha P_\infty)$ is a

$$[q^{r-1}(uq-u+1), \sum_{i=0}^{u-1} \max\left\{ \left\lfloor \frac{\alpha - iq^{r-1}}{u} \right\rfloor + 1, 0 \right\}, \geq q^{r-1}(uq-u+1) - \alpha]_{q^r}$$

code.

Taking q to be a power of 2 and applying Lemma 20 to the code above yields a small-bias set as detailed in the next result.

Theorem 21. *There exists an ϵ-biased set $X \subseteq \mathbb{F}_2^{r \log q \sum_{i=0}^{u-1} \max\left\{ \left\lfloor \frac{\alpha - iq^{r-1}}{u} \right\rfloor + 1, 0 \right\}}$ with $|X| = q^{2r-1}(uq-u+1)$ and $\epsilon = \frac{\alpha}{q^{r-1}(uq-u+q)}$ for every positive integer $\alpha < q^{r-1}(uq-u+1)$, $r \geq 2$, q a power of 2, and $u | \frac{q^r-1}{q-1}$.*

Next, we give the explicit description of the small-bias sets in Theorem 21. Consider the function field $\mathbb{F}_{2^s}(x, y)/\mathbb{F}_{2^s}$ where $\mathbb{F}_{2^s} = \mathbb{F}_2(\gamma)$. Let $G = \alpha P_\infty$ and D be the sum of all places of degree one other than P_∞. By Theorem 13, we can construct a generator matrix M for the corresponding algebraic geometry code $C_{\mathcal{L}}(D, G)$. Furthermore, we consider the Walsh-Hadamard code C_s, which has generator matrix M', and denote the concatenation of $C_{\mathcal{L}}(D, G)$ and C_s by C.

Then, define the map φ as follows:

$$\begin{aligned} \varphi: \ 1 &\mapsto Row_1 M' \\ \gamma &\mapsto Row_2 M' \\ \gamma^2 &\mapsto Row_3 M' \\ &\vdots \\ \gamma^{s-1} &\mapsto Row_s M. \end{aligned}$$

We may extend this map to $\mathbb{F}_{2^s}$ by $\varphi(a+b) = \varphi(a) + \varphi(b)$ for $a, b \in \mathbb{F}_{2^s}$. This map may be further extended to $\mathbb{F}_{2^s}^n$ by $\varphi(a_1, a_2, \ldots, a_n) = (\varphi(a_1), \varphi(a_2), \ldots, \varphi(a_n))$. Now, consider the set of vectors

$$S = \{Row_1 M, \gamma Row_1 M, \ldots, \gamma^{s-1} Row_1 M, \ldots, Row_k M, \gamma Row_k M, \ldots, \gamma^{s-1} Row_k M\}.$$

Then, the rows of the generator matrix for the concatenated code C are the images under φ applied to S, that is, the generator matrix for C is

$$\begin{bmatrix} \varphi(Row_1 M) \\ \varphi(\gamma Row_1 M) \\ \vdots \\ \varphi(\gamma^{s-1} Row_1 M) \\ \vdots \\ \varphi(Row_k M) \\ \vdots \\ \varphi(\gamma^{s-1} Row_k M) \end{bmatrix}.$$

In other words, if

$$M := \begin{bmatrix} f_1(Q_1) & f_1(Q_2) & \cdots & f_1(Q_n) \\ f_2(Q_1) & f_2(Q_2) & \cdots & f_2(Q_n) \\ \vdots & \vdots & & \vdots \\ f_k(Q_1) & f_k(Q_2) & \cdots & f_k(Q_n) \end{bmatrix}$$

is a generator matrix for $C_{\mathcal{L}}(D, G)$, then a generator matrix M_1 for the concatenated code C is

$$\begin{bmatrix} \varphi(f_1(Q_1)) & \varphi(f_1(Q_2)) & \dots & \varphi(f_1(Q_n)) \\ \varphi(\gamma f_1(Q_1)) & \varphi(\gamma f_1(Q_2)) & \dots & \varphi(\gamma f_1(Q_n)) \\ \vdots & \vdots & & \vdots \\ \varphi(\gamma^{s-1} f_1(Q_1)) & \varphi(\gamma^{s-1} f_1(Q_2)) & \dots & \varphi(\gamma^{s-1} f_1(Q_n)) \\ \vdots & \vdots & & \vdots \\ \varphi(f_k(Q_1)) & \varphi(f_k(Q_2)) & \dots & \varphi(f_k(Q_n)) \\ \vdots & \vdots & & \vdots \\ \varphi(\gamma^{s-1} f_k(Q_1)) & \varphi(\gamma^{s-1} f_k(Q_2)) & \dots & \varphi(\gamma^{s-1} f_k(Q_n)) \end{bmatrix}.$$

Example 8. [5] Take F to be the Hermitian function field defined by $y^q + y = x^{q+1}$ over $\mathbb{F}_{q^2}$, where $q^2 = 2^s$. The Hermitian code $C_{\mathcal{L}}(D, \alpha P_\infty)$ gives rise to a $\frac{\alpha}{q^3}$-biased set $X \subseteq \mathbb{F}_2^{s\ell(\alpha P_\infty)}$ with $|X| = q^5$. This construction improves upon previous explicit constructions when ϵ is roughly in the range $[k^{-1.5}, k^{-.5}]$.

Every ϵ-biased set $X \subseteq \mathbb{F}_2^k$ satisfies $\left|X\right| \geq \min\left\{\frac{k}{\epsilon^2 \log \frac{1}{\epsilon}}, 2^k\right\}$, see [5]. With this in mind, we fix k and ϵ and consider $|X|$ for the construction given in Theorem 21. Notice that the small-bias set X given in Example 7 has $|X| = \mathcal{O}\left(\frac{k^2}{\epsilon^2}\right)$.

Theorem 22. *For all k and ϵ such that $\frac{\epsilon}{\left(\log \frac{1}{\epsilon}\right)^{\frac{1}{\sqrt{l}}}} \leq k^{\frac{-1}{\sqrt{l}}}$ for some integer $l \geq 4$, there exists an ϵ- biased set $X \subseteq \mathbb{F}_2^{\Omega(k)}$ with cardinality $|X| = \mathcal{O}\left(\left(\frac{k}{\epsilon^{l-\sqrt{l}} \log \frac{1}{\epsilon}}\right)^{\frac{l+1}{l}}\right)$.*

Proof. Fix k and ϵ so that $\frac{\epsilon}{\left(\log \frac{1}{\epsilon}\right)^{\frac{1}{\sqrt{l}}}} \leq k^{\frac{-1}{\sqrt{l}}}$ for some positive integer $l \geq 4$. Choose

$$q \in \left[\left(\frac{k}{\epsilon^{l-\sqrt{l}} \log \frac{1}{\epsilon}} \right)^{\frac{1}{l}}, 2 \left(\frac{k}{\epsilon^{l-\sqrt{l}} \log \frac{1}{\epsilon}} \right)^{\frac{1}{l}} \right]$$

to be a power of 2, say $q = 2^s$. Then

$$\begin{aligned} \frac{1}{q} &\geq \frac{1}{2} \left(\frac{\epsilon^{l-\sqrt{l}} \log \frac{1}{\epsilon}}{k} \right)^{\frac{1}{l}} \\ &= \frac{1}{2} \epsilon^{\frac{l-\sqrt{l}}{l}} \left(\frac{\log \frac{1}{\epsilon}}{k} \right)^{\frac{1}{l}} \\ &\geq \frac{1}{2} \epsilon^{\frac{l-\sqrt{l}}{l}} \epsilon^{\frac{1}{\sqrt{l}}} = \frac{1}{2} \epsilon. \end{aligned}$$

We also have that

$$\frac{1}{q} \leq \frac{\epsilon^{\frac{l-\sqrt{l}}{l}} \left(\log \frac{1}{\epsilon} \right)^{\frac{1}{l}}}{k^{\frac{1}{l}}} \leq \epsilon^{\frac{l-\sqrt{l}}{l}}$$

since $\left(\frac{\log \frac{1}{\epsilon}}{k} \right)^{\frac{1}{\sqrt{l}}} \leq 1$. Hence,

$$\left(\frac{1}{q} \right)^{\frac{l}{l-\sqrt{l}}} \leq \epsilon \leq \frac{2}{q},$$

and

$$\log \frac{q}{2} \leq \log \frac{1}{\epsilon} \leq \left(\frac{l}{l-\sqrt{l}} \right) \log q.$$

It follows that $\log \frac{1}{\epsilon} = \Theta \left(\log q \right)$.

Set $r = \left\lfloor \frac{l+2}{3} \right\rfloor$, and let $\alpha = \frac{\epsilon q^{2r-1}}{2}$. Consider the norm-trace function field over $F/\mathbb{F}_{q^r}$. We claim that the set X of columns of a generator matrix for $C_{\mathcal{L}}(D, \alpha P_\infty)$ is an ϵ-biased set with $X \subseteq \mathbb{F}_2^{\Omega(k)}$ and $|X| = \mathcal{O}\left(\left(\frac{k}{\epsilon^{l-\sqrt{l}} \log \frac{1}{\epsilon}} \right)^{\frac{l+1}{l}} \right)$.

First, we prove that $X \subseteq \mathbb{F}_2^{\Omega(k)}$. Let $u = \frac{q^r-1}{q-1}$, and set $m = \left\lfloor \frac{\alpha}{q^{r-1}} \right\rfloor$. As stated in Equation (3.1),

$$\ell \left(\alpha P_\infty \right) = \sum_{i=0}^{u-1} \max \left\{ \left\lfloor \frac{\alpha - i q^{r-1}}{u} \right\rfloor + 1, 0 \right\}$$

which gives

$$\ell\left(\alpha P_\infty\right) \geq \sum_{i=0}^{m} \frac{\alpha - iq^{r-1}}{u}$$

since $m \leq u-1$. Simplifying, we see that

$$\ell\left(\alpha P_\infty\right) \geq \frac{\alpha}{u}(m+1) - \frac{q^{r-1}}{u}\frac{m(m+1)}{2} \geq \frac{1}{2}\frac{\alpha}{u}(m+1)$$

as $m \leq \frac{\alpha}{q^r-1}$. It then follows that

$$\ell\left(\alpha P_\infty\right) \geq \frac{1}{2}\left(\frac{\alpha}{u}\right)^2 \geq \frac{1}{32}q^l\epsilon^2.$$

As a result,

$$\ell\left(\alpha P_\infty\right) \geq \frac{k}{32\log\frac{1}{\epsilon}} \geq \frac{l-\sqrt{l}}{32l}\frac{k}{\log q},$$

and $\ell\left(\alpha P_\infty\right) \in \Omega\left(\frac{k}{\log q}\right)$. This implies $X \subseteq \mathbb{F}_2^{\Omega(k)}$.

Next, we note that X is $\frac{\epsilon}{2}$-biased as $\frac{\alpha}{n} = \frac{\epsilon}{2}$. Because $\epsilon > \frac{\epsilon}{2}$, X is certainly ϵ-biased by definition.

Finally, it follows from Theorem 21 that $\mid X \mid = q^{3r-1}$. Therefore, $|X| = \mathcal{O}\left(\left(\frac{k}{\epsilon^{l-\sqrt{l}}\log\frac{1}{\epsilon}}\right)^{\frac{l+1}{l}}\right)$.

□

By taking $l = 4$ in the previous theorem, one may recover the following result due to Ben-Aroya and Ta-Shma.

Corollary 23. *[5] For all k and ϵ such that $\frac{\epsilon}{\sqrt{\log\frac{1}{\epsilon}}} \leq \frac{1}{\sqrt{k}}$, there exists an ϵ- biased set $X \subseteq \mathbb{F}_2^{\Omega(k)}$ with cardinality $|X| = \mathcal{O}\left(\left(\frac{k}{\epsilon^2\log\frac{1}{\epsilon}}\right)^{\frac{5}{4}}\right)$.*

3.3 Examples

In this section, we illustrate the construction of a small-bias set from a norm-trace code.

Example 9. Consider the function field $F := \mathbb{F}_8(x, y)/\mathbb{F}_8$ where

$$y^4 + y^2 + y = x^7.$$

Let $G = 15P_\infty$, and let D be the sum of all places of F of degree one other than those in the support of G. Thus, $C_{\mathcal{L}}(D, G)$ has length 32. By [30], a basis for $\mathcal{L}(G)$ is $\{1, x, x^2, x^3, y, y^2, xy, x^2y\}$. Thus, a generator matrix for $C_{\mathcal{L}}(D, G)$ is

$$M := \begin{bmatrix} 1(P_1) & 1(P_2) & \cdots & 1(P_{32}) \\ x(P_1) & x(P_2) & \cdots & x(P_{32}) \\ x^2(P_1) & x^2(P_2) & \cdots & x^2(P_{32}) \\ x^3(P_1) & x^3(P_2) & \cdots & x^3(P_{32}) \\ y(P_1) & y(P_2) & \cdots & y(P_{32}) \\ y^2(P_1) & y^2(P_2) & \cdots & y^2(P_{32}) \\ xy(P_1) & xy(P_2) & \cdots & xy(P_{32}) \\ x^2y(P_1) & x^2y(P_2) & \cdots & x^2y(P_{32}) \end{bmatrix}.$$

Using the above information, we can construct a small bias set by concatenating $C_{\mathcal{L}}(D, G)$ with the appropriate Walsh-Hadamard code. Let $\mathbb{F}_8 = \mathbb{F}_2(\gamma)$ where γ is a root of $x^3 + x + 1$. Let M' be a generator matrix for the Walsh-Hadamard code C_3, that is,

$$M' := \begin{bmatrix} 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{bmatrix}.$$

Then, the rows of the generator matrix for the concatenated code are the images under φ applied to

$$S = \{Row_1 M, \gamma Row_1 M, \gamma^2 Row_1 M, \ldots, Row_7 M, \gamma Row_7 M, \gamma^2 Row_7 M\}.$$

The elements of the associated small-bias set are the columns of the following generator

matrix for the concatenated code.

$$\begin{bmatrix}
\varphi(1(P_1)) & \varphi(1(P_2)) & \cdots & \varphi(1(P_{32})) \\
\varphi(\gamma(P_1)) & \varphi(\gamma(P_2)) & \cdots & \varphi(\gamma(P_{32})) \\
\varphi(\gamma^2(P_1)) & \varphi(\gamma^2(P_2)) & \cdots & \varphi(\gamma^2(P_{32})) \\
\varphi(x(P_1)) & \varphi(x(P_2)) & \cdots & \varphi(x(P_{32})) \\
\varphi(\gamma x(P_1)) & \varphi(\gamma x(P_2)) & \cdots & \varphi(\gamma x(P_{32})) \\
\varphi(\gamma^2 x(P_1)) & \varphi(\gamma^2 x(P_2)) & \cdots & \varphi(\gamma^2 x(P_{32})) \\
\varphi(x^2(P_1)) & \varphi(x^2(P_2)) & \cdots & \varphi(x^2(P_{32})) \\
\varphi(\gamma x^2(P_1)) & \varphi(\gamma x^2(P_2)) & \cdots & \varphi(\gamma x^2(P_{32})) \\
\varphi(\gamma^2 x^2(P_1)) & \varphi(\gamma^2 x^2(P_2)) & \cdots & \varphi(\gamma^2 x^2(P_{32})) \\
\varphi(x^3(P_1)) & \varphi(x^3(P_2)) & \cdots & \varphi(x^3(P_{32})) \\
\varphi(\gamma x^3(P_1)) & \varphi(\gamma x^3(P_2)) & \cdots & \varphi(\gamma x^3(P_{32})) \\
\varphi(\gamma^2 x^3(P_1)) & \varphi(\gamma^2 x^3(P_2)) & \cdots & \varphi(\gamma^2 x^3(P_{32})) \\
\varphi(y(P_1)) & \varphi(y(P_2)) & \cdots & \varphi(y(P_{32})) \\
\varphi(\gamma y(P_1)) & \varphi(\gamma y(P_2)) & \cdots & \varphi(\gamma y(P_{32})) \\
\varphi(\gamma^2 y(P_1)) & \varphi(\gamma^2 y(P_2)) & \cdots & \varphi(\gamma^2 y(P_{32})) \\
\varphi(y^2(P_1)) & \varphi(y^2(P_2)) & \cdots & \varphi(y^2(P_{32})) \\
\varphi(\gamma y^2(P_1)) & \varphi(\gamma y^2(P_2)) & \cdots & \varphi(\gamma y^2(P_{32})) \\
\varphi(\gamma^2 y^2(P_1)) & \varphi(\gamma^2 y^2(P_2)) & \cdots & \varphi(\gamma^2 y^2(P_{32})) \\
\varphi(xy(P_1)) & \varphi(xy(P_2)) & \cdots & \varphi(xy(P_{32})) \\
\varphi(\gamma xy(P_1)) & \varphi(\gamma xy(P_2)) & \cdots & \varphi(\gamma xy(P_{32})) \\
\varphi(\gamma^2 xy(P_1)) & \varphi(\gamma^2 xy(P_2)) & \cdots & \varphi(\gamma^2 xy(P_{32})) \\
\varphi(x^2 y(P_1)) & \varphi(x^2 y(P_2)) & \cdots & \varphi(x^2 y(P_{32})) \\
\varphi(\gamma x^2 y(P_1)) & \varphi(\gamma x^2 y(P_2)) & \cdots & \varphi(\gamma x^2 y(P_{32})) \\
\varphi(\gamma^2 x^2 y(P_1)) & \varphi(\gamma^2 x^2 y(P_2)) & \cdots & \varphi(\gamma^2 x^2 y(P_{32}))
\end{bmatrix}.$$

Example 10. Consider the function field $F := \mathbb{F}_{16}(x, y)/\mathbb{F}_{16}$ where

$$y^8 + y^4 + y^2 + y = x^{15}.$$

Let $G = 23P_\infty$, and let D be the sum of all places of F of degree one other than those in the support of G. Thus, $C_{\mathcal{L}}(D, G)$ has length 128. By [30], a basis for $\mathcal{L}(G)$ is $\{1, x, y, xy, x^2\}$. Thus, a generator matrix for $C_{\mathcal{L}}(D, G)$ is

$$M := \begin{bmatrix} 1(P_1) & 1(P_2) & \cdots & 1(P_{128}) \\ x(P_1) & x(P_2) & \cdots & x(P_{128}) \\ x^2(P_1) & x^2(P_2) & \cdots & x^2(P_{128}) \\ y(P_1) & y(P_2) & \cdots & y(P_{128}) \\ xy(P_1) & xy(P_2) & \cdots & xy(P_{128}) \end{bmatrix}.$$

Using the above information, we can construct a small bias set by concatenating $C_{\mathcal{L}}(D, G)$ with the appropriate Walsh-Hadamard code. Let $\mathbb{F}_{16} = \mathbb{F}_2(\gamma)$ where γ is a root of $x^4 + x^3 + 1$. Let M' be a generator matrix for the Walsh-Hadamard code C_4, that is,

$$M' := \begin{bmatrix} 0 & 1 & 0 & 0 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}.$$

Then, the rows of the generator matrix for the concatenated code are the images under φ applied to

$$S = \{Row_1 M, \gamma Row_1 M, \gamma^2 Row_1 M, \ldots, Row_7 M, \gamma Row_7 M, \gamma^2 Row_7 M\}.$$

The columns of this generator matrix for the concatenated code are the elements of the associated small-bias set. Thus, the generator matrix can be found in a similar method to the previous example.

Chapter 4

Weierstrass semigroups of places on a function field

Let q be a power of a prime and r be an integer with $r \geq 2$. Consider the function field $\mathbb{F}_{q^r}(x,y)/\mathbb{F}_{q^r}$ where

$$N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(x) = Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(y),$$

meaning the norm of x with respect to the extension $\mathbb{F}_{q^r}/\mathbb{F}_q$ is equal to the trace of y with respect to the extension $\mathbb{F}_{q^r}/\mathbb{F}_q$. This function field is called the norm-trace function field. If $r = 2$, then the norm-trace function field coincides with the well-studied Hermitian function field. The norm-trace function field was first studied by Geil in [12] where he considered evaluation codes and one-point algebraic geometry codes constructed from this function field. More recently, Munuera, Tizziotti, and Torres [31] examined two-point algebraic geometry codes and associated Weierstrass semigroups on the norm-trace function field.

Given an algebraic function field $F/\mathbb{F}$, where $\mathbb{F}$ is a finite field, and distinct places

$P_1, \ldots, P_m$ of F of degree one, the Weierstrass semigroup of the m-tuple $(P_1, \ldots, P_m)$ is

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

where $(f)_\infty$ denotes the divisor of poles of f and $\mathbb{N}$ denotes the set of nonnegative integers. The Weierstrass gap set $G(P_1, \ldots, P_m)$ of the m-tuple $(P_1, \ldots, P_m)$ is defined by

$$G(P_1, \ldots, P_m) = \mathbb{N}^m \setminus H(P_1, \ldots P_m).$$

The semigroup $H(P)$ and the associated gap set $G(P)$ are objects of classical study. While we are mostly interested in $H(P_1, \ldots P_m)$ and $G(P_1, \ldots P_m)$ with $m > 1$, the following theorem is quite useful.

Theorem 24. *[35, Theorem I.6.7] (Weierstrass gap theorem)*

Suppose that F/K has genus $g > 0$ and P is a place of degree one. Then, there are exactly g gap numbers $i_1 < \cdots < i_g$ at P, and

$$i_1 = 1 \text{ and } i_g \leq 2g - 1.$$

In this chapter, we determine the minimal generating set of the Weierstrass semigroup $H\left(P_\infty, P_{0b_2}, \ldots, P_{0b_m}\right)$ on the norm-trace function field for any m, $2 \leq m \leq q^{r-1} + 1$. This chapter is organized as follows. This section concludes with notation utilized in the paper. Section 4.1 contains relevant background on the norm-trace function field. The main result is found in Section 4.2. This chapter concludes with examples given in Section 4.3

Notation. The set of positive integers is denoted $\mathbb{Z}_+$. Define a partial order $\preceq$ on $\mathbb{Z}^m$ by $(n_1, \ldots, n_m) \preceq (p_1, \ldots, p_m)$ if and only if $n_i \leq p_i$ for all i, $1 \leq i \leq m$. When comparing elements of $\mathbb{Z}^m$, we will always do so with respect to the partial order $\preceq$. We use the notation $n \prec p$ to mean $n \preceq p$ and $n \neq p$.

4.1 Preliminaries on the norm-trace function field

In this section, we review the necessary background on the norm-trace function field; additional details may be found in [12].

Consider the norm-trace function field $F := \mathbb{F}_{q^r}(x,y)/\mathbb{F}_{q^r}$ which has defining equation

$$y^{q^{r-1}} + y^{q^{r-2}} + \cdots + y = x^{a+1}$$

where $a := \frac{q^r-1}{q-1} - 1$, q is a power of a prime, and $r \geq 2$ is an integer. The genus of $F/\mathbb{F}_{q^r}$ is $g = \frac{a\left(q^{r-1}-1\right)}{2}$. For each $\alpha \in \mathbb{F}_{q^r}$, there are q^{r-1} elements $\beta \in \mathbb{F}_{q^r}$ such that

$$N_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) = Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\beta). \tag{4.1}$$

For every pair $(\alpha,\beta) \in \mathbb{F}_{q^r}^2$ satisfying Equation (4.1), there is a place $P_{\alpha\beta}$ of F of degree one which is the common zero of $x-\alpha$ and $y-\beta$. In fact, the places of F of degree one are precisely these $P_{\alpha\beta}$ and P_∞, the common pole of x and y. In particular, there are q^{r-1} places P_{0b} with $b \in \mathcal{B}$ where

$$\mathcal{B} := \left\{ b \in \mathbb{F}_{q^r} : Tr_{\mathbb{F}_{q^r}/\mathbb{F}_q}(b) = 0 \right\}.$$

In determining the Weierstrass semigroups $H(P_\infty)$ and $H(P_{0b})$, for $b \in \mathcal{B}$, on the norm-trace function field, the following principal divisors are quite useful:

$$(x) = \sum_{b\in\mathcal{B}} P_{0b} - q^{r-1}P_\infty$$

and for any $b \in \mathcal{B}$,

$$(y-b) = (a+1)P_{0b} - (a+1)P_\infty.$$

Combining these with the fact that $|G(P)| = g$ for any place P of degree one, it can be

shown that gap set of the infinite place is

$$G\left(P_\infty\right)=\left\{\begin{array}{cc}&1\leq j\leq i\leq a-s \text{ and}\\ \left(q^{r-1}-i+j-1\right)(a+1)-jq^{r-1}: & (s-1)\left(q-1\right)\leq i-j<s\left(q-1\right)\\ &\text{where } 1\leq s\leq a+1-q^{r-1}\end{array}\right\}$$

and the gap set of any place P_{0b} where $b\in\mathcal{B}$ is

$$G(P_{0b})=\left\{\begin{array}{cc}&1\leq j\leq i\leq a-s \text{ and}\\ (i-j)(a+1)+j: & (s-1)(q-1)\leq i-j<s(q-1)\\ &\text{where } 1\leq s\leq a+1-q^{r-1}\end{array}\right\}.$$

Moreover, each element of the gap set $G\left(P_\infty\right)$ has a unique representation of the form above; specifically, if

$$(q^{r-1}-i+j-1)(a+1)-jq^{r-1}=(q^{r-1}-i'+j'-1)(a+1)-j'q^{r-1},$$

where $1\leq j,j'\leq a-1$, then

$$i'=i \text{ and } j'=j.$$

A similar fact holds for elements of the gap set $G\left(P_{0b}\right)$ where $b\in\mathcal{B}$. Additional details may be found in [12, 29, 31].

4.2 Weierstrass semigroups on the norm-trace function field

In this section, we determine the minimal generating set of $H\left(P_\infty,P_{0b_2},\ldots,P_{0b_m}\right)$ on the norm-trace function field for any m, $2\leq m\leq q^{r-1}$, and any distinct $b_i\in\mathcal{B}$.

Definition 24. Let $P_1, \ldots, P_m$ be m distinct places of degree one of an algebraic function field of $F/\mathbb{F}$. Set $\Gamma(P_1) := H(P_1)$; for $m \geq 2$, set

$$\Gamma(P_1, \ldots, P_m) := \left\{ \mathbf{n} \in \mathbb{Z}_+^m : \begin{array}{c} \mathbf{n} \text{ is minimal in } \{\mathbf{p} \in H(P_1, \ldots, P_m) : p_i = n_i\} \\ \text{for some } i, 1 \leq i \leq m \end{array} \right\}.$$

In [27] it is shown that if $2 \leq m \leq |\mathbb{F}|$, then $H(P_1, \ldots, P_m) =$

$$\left\{ \text{lub}\{\mathbf{u_1}, \ldots, \mathbf{u_m}\} : \begin{array}{c} \mathbf{u_i} \in \mathbf{\Gamma}(\mathbf{P_1}, \ldots, \mathbf{P_m}) \text{ or } (\mathbf{u_{i_1}}, \ldots, \mathbf{u_{i_k}}) \in \mathbf{\Gamma}(\mathbf{P_{i_1}}, \ldots, \mathbf{P_{i_k}}) \\ \text{for some } \{i_1, \ldots, i_m\} = \{1, \ldots, m\} \text{ such that } i_1 < \cdots < i_k \\ \text{and } u_{i_{k+1}} = \cdots = u_{i_m} = 0 \text{ for some } 1 \leq k < m \end{array} \right\}$$

where

$$\text{lub}\{\mathbf{u_1}, \ldots, \mathbf{u_m}\} = (\max\{\mathbf{u_{1_1}}, \ldots, \mathbf{u_{m_1}}\}, \ldots, \max\{\mathbf{u_{1_m}}, \ldots, \mathbf{u_{m_m}}\}) \in \mathbb{N}^{\mathbf{m}}$$

is least upper bound of the vectors $\mathbf{u_1}, \ldots, \mathbf{u_m} \in \mathbb{N}^{\mathbf{m}}$. The set $\Gamma(P_1, \ldots, P_m)$ is called the minimal generating set of the Weierstrass semigroup $H(P_1, \ldots, P_m)$. Hence, to determine the entire Weierstrass semigroup $H(P_1, \ldots, P_m)$, one only needs to determine the minimal generating sets $\Gamma(P_{i_1}, \ldots, P_{i_k})$. The next two lemmas aid in finding such sets.

Lemma 25. *[27] Let $F/\mathbb{F}$ be an algebraic function field where $\mathbb{F}$ is a finite field. Suppose $P_1, \ldots, P_m$ are distinct places of $F/\mathbb{F}$ of degree one and $2 \leq m \leq |\mathbb{F}|$. Then*

1. $\Gamma(P_1, \ldots, P_m) \subseteq G(P_1) \times \cdots \times G(P_m)$.

2. $$\Gamma(P_1, \ldots, P_m) = \left\{ \mathbf{n} \in \mathbb{Z}_+^m : \begin{array}{c} \mathbf{n} \text{ is minimal in} \\ \{\mathbf{p} \in H(P_1, \ldots, P_m) : p_i = n_i\} \\ \text{for all } i, 1 \leq i \leq m \end{array} \right\}.$$

The following result details how the minimal generating set $\Gamma(P_1, \ldots, P_m)$ is related to dimensions of Riemann-Roch spaces $\mathcal{L}(P_1, \ldots, P_m)$.

Lemma 26. *[27, Proposition 9] For $1 \leq m \leq |\mathbb{F}|$ and $\boldsymbol{\alpha} \in \mathbb{N}^m$, the following are equivalent:*

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

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

for all j, $1 \leq j \leq r$.

We aim to find $\Gamma\left(P_\infty, P_{0b_2}, \ldots, P_{0b_m}\right)$ on the norm-trace function field. The case $m = 2$ appears in [31] and is recorded here as the next lemma.

Lemma 27. *[31] Let $b \in \mathcal{B}$. The minimal generating set of the Weierstrass semigroup of the pair (P_∞, P_{0b}) of places on the norm-trace function field over $\mathbb{F}_{q^r}$ is*

$$\Gamma\left(P_\infty, P_{0b}\right) = \left\{ \begin{array}{cc} & 1 \leq j \leq i \leq a - s, \\ v_{ij}: & (s-1)\,(q-1) \leq i - j \leq s\,(q-1) - 1 \\ & \text{for some } 1 \leq s \leq a + 1 - q^{r-1} \end{array} \right\}$$

where

$$v_{ij} := \left((a+1)\left(q^{r-1} - i + j - 1\right) - jq^{r-1}, (a+1)\,(i-j) + j\right).$$

Utilizing the two lemmas above, we next prove the main result of this section.

Theorem 28. *Suppose $2 \leq m \leq q^{r-1} + 1$. The minimal generating set of the Weierstrass semigroup of the m-tuple $(P_\infty, P_{0b_2}, \ldots, P_{0b_m})$ of places of the norm-trace function field over*

$\mathbb{F}_{q^r}$ *is*

$$\Gamma(P_\infty, P_{0b_2}, \ldots, P_{0b_m}) = \left\{ \gamma_{j,\mathbf{t}} : \begin{array}{l} \sum_{k=2}^{m} t_k = i-j+1, t_k \in \mathbb{Z}_+, 1 \le j \le i \le a-s, \\ (s-1)(q-1) \le i-j \le s(q-1)-1 \\ \textit{where } 1 \le s \le a+1-q^{r-1} \end{array} \right\}$$

where

$$\gamma_{j,\mathbf{t}} = \left(\left(q^{r-1} - \sum_{k=2}^{m} t_k \right)(a+1) - jq^{r-1}, (t_2-1)(a+1)+j, \ldots, (t_m-1)(a+1)+j \right).$$

Proof. For $2 \le m \le q^{r-1}+1$, set

$$S_m := \left\{ \gamma_{j,\mathbf{t}} : \begin{array}{l} \sum_{k=2}^{m} t_k = i-j+1, t_i \in \mathbb{Z}_+, 1 \le j \le i \le a-s, \\ (s-1)(q-1) \le i-j \le s(q-1)-1 \\ \text{where } 1 \le s \le a+1-q^{r-1} \end{array} \right\}.$$

When convenient, we write $H_m := H(P_\infty, P_{0b_2}, \ldots, P_{0b_m})$ and $\Gamma_m := \Gamma(P_\infty, P_{0b_2}, \ldots, P_{0b_m})$, $m \ge 2$. We prove that $S_m = \Gamma_m$ by induction on m. By Lemma 27, $S_2 = \Gamma_2$. Assume that $\Gamma_l = S_l$ for $2 \le l \le m-1$. First, we show that $S_m \subseteq \Gamma_m$.

Let $s := \gamma_{j,\mathbf{t}} \in S_m$. Hence,

$$s_1 = \left(q^{r-1} - \sum_{i=2}^{m} t_i \right)(a+1) - jq^{r-1},$$

and for $2 \le i \le m$,

$$s_i = (t_i - 1)(a+1) + j.$$

Then $s \in H_m$, since $\left(\frac{x^{a+1-j}}{\prod_{i=2}^{m} (y-b_i)^{t_i}} \right)_\infty =$

$$\left(\left(q^{r-1} - \sum_{i=2}^{m} t_i \right) (a+1) - jq^{r-1} \right) P_\infty + \sum_{i=2}^{m} ((t_i - 1)(a+1) + j) P_{0b_i}.$$

It remains to show that $s \in \Gamma_m$.

Let $Q_1 := \{p \in H_m : p_1 = s_1\}$. Then $s \in Q_1$. We claim that s is minimal in Q_1. Suppose not; that is, suppose there exists $w \in Q_1$ such that

$$w \prec s.$$

Then there exists $f \in F$ with divisor

$$(f) = A - (w_1 P_\infty + w_2 P_{0b_2} + \cdots + w_m P_{0b_m})$$

where A is effective. Clearly, $w_i \leq s_i$ for $1 \leq i \leq m$ and $w_i < s_i$ for some $2 \leq i \leq m$. We may assume $w_2 < s_2$ as a similar argument holds for any other i. Then

$$w_2 = (t_2 - 1)(a+1) + j - k$$

for some $k \in \mathbb{Z}^+$.

Suppose that $j \leq k$. Notice that

$$\left(f\,(y-b_2)^{t_2-1}\right) = A' - (w_1 + (t_2-1)(a+1))P_\infty - (j-k)\,P_{0b_2} - \sum_{k=3}^{m} w_k P_{0b_k}$$

where A' is an effective divisor. Then

$$v := (w_1 + (t_2 - 1)(a+1), w_3, \ldots, w_m) \in H\left(P_\infty, P_{0b_3}, \ldots, P_{0b_m}\right)$$

since $j - k \leq 0$. Now, since

$$w_1 + (t_2 - 1)(a+1) = \left(q^{r-1} - \left(1 + \sum_{i=3}^{m} t_i\right)\right)(a+1) - jq^{r-1},$$

we obtain that

$$\begin{aligned} v &\preceq \left(\left(q^{r-1} - \sum_{i=3}^{m} t_i'\right)(a+1) - jq^{r-1}, (t_3' - 2)(a+1) + j, \ldots, (t_m' - 1)(a+1) + j\right) \\ &\prec \gamma_{j,(t_3', \ldots, t_m')}, \end{aligned}$$

where $t_3' = t_3 + 1$ and $t_i' = t_i$ for $4 \leq i \leq m$. We claim that

$$\gamma_{j,(t_3', \ldots, t_m')} \in \Gamma\left(P_\infty, P_{0b_3}, \ldots, P_{0b_m}\right).$$

To see this, let $i' = \sum_{i=3}^{m} t_i' + j - 1$. Then, $i' - j + 1 = \sum_{i=3}^{m} t_i'$. First, note that $\sum_{i=3}^{m} t_i' \leq \sum_{i=2}^{m} t_i$. Thus, $i' - j + 1 \leq i - j + 1$. Hence, $i' \leq i \leq a - s$ and $i' - j \leq i - j$. Thus, we can find an s_l such that $1 \leq s_l \leq s \leq a + 1 - q^{r-1}$ and $(s_l - 1)(q-1) \leq i - j \leq s_l(q-1) - 1$. Furthermore, $i' \leq a - s \leq a - s_l$. Also, $i' + 1 = \sum_{i=3}^{m} t_i' + j$ implies $i' > j$. Thus, we have that

$$v \prec \gamma_{j,(t_3', \ldots, t_m')}$$

and

$$\gamma_{j,(t_3', \ldots, t_m')} \in \Gamma\left(P_\infty, P_{0b_3}, \ldots, P_{0b_m}\right)$$

which is a contradiction. Hence, it must be that $j > k$.

Now, note that $\left(fx^{j-k}(y-b_2)^{t_2-1}\right) =$

$$A'' - (w_1 + (t_2-1)(a+1) + (j-k)q^{r-1})P_\infty - \sum_{i=3}^{m}(w_i - (j-k))P_{0b_i}.$$

where A'' is an effective divisor. Set

$$v := \left(\left(q^{r-1} - \sum_{i=3}^{m} t_i - 1\right)(a+1) - kq^{r-1}, w_3 - (j-k), \ldots, w_m - (j-k)\right).$$

Then $v \in H_m$. An argument similar to that above shows

$$v \prec \gamma_{k,(t_3',\ldots,t_m')},$$

where $t_3' = t_3 + 1$ and $t_i' = t_i$ for $4 \leq i \leq m$, and

$$\gamma_{k,(t_3',\ldots,t_m')} \in \Gamma\left(P_\infty, P_{0b_3}, \ldots, P_{0b_m}\right),$$

which is a contradiction. This proves that s is minimal in Q_1. Hence, $s \in \Gamma_m$, and it follows that $S_m \subseteq \Gamma_m$.

Next, we show that $\Gamma_m \subseteq S_m$. Let $n \in \Gamma_m$. By Lemma 25(1),

$$n \in G(P_\infty) \times G(P_{0b_2}) \times \cdots \times G(P_{0b_m}).$$

According to Lemma 27, this implies

$$\begin{aligned} n_1 &= (a+1)(q^{r-1} - i_1 + j_1 - 1) - j_1 q^{r-1}, \text{ and} \\ n_l &= (a+1)(i_l - j_l) + j_l, \text{ for } 2 \leq l \leq m, \end{aligned}$$

where for all l, $2 \leq l \leq m$,

$$\begin{aligned} &1 \leq j_l \leq i_l \leq a - s_l, \\ &(s_l - 1)(q-1) \leq i_l - j_l \leq s_l(q-1) - 1, \text{ for some } s_l, \\ &1 \leq s_l \leq a + 1 - q^{r-1}. \end{aligned}$$

We may assume without loss of generality that

$$j_2 = \min\{j_l : 2 \leq l \leq m\}$$

since the argument is similar for any j_l where $j_l = \min\{j_l : 2 \leq l \leq m\}$. Then there exists $h \in F$ with

$$(h)_\infty = n_1 P_\infty + \sum_{k=2}^{m} n_k P_{0b_k}.$$

This implies $\left(h \prod_{k=3}^{m} (y - b_k)^{i_k - j_k + 1}\right)_\infty =$

$$\left(n_1 + (a+1) \sum_{k=3}^{m} (i_k - j_k) + (a+1)(m-2) \right) P_\infty - n_2 P_{0b_2},$$

and

$$v := \left(n_1 + (a+1) \sum_{k=3}^{m} (i_k - j_k + 1), n_2 \right) \in H\left(P_\infty, P_{0b_2}\right).$$

By Lemma 25(2), there exists $u \in \Gamma_2$ such that $u \preceq v$ and $u_2 = n_2$. Lemma 27 implies

$$u_1 = (a+1)(q^{r-1} - i_2 + j_2 - 1) - j_2 q^{r-1}.$$

Furthermore, $u_1 > n_1$; otherwise, $(u_1, u_2, 0, \ldots, 0) \prec n$, which contradicts the minimality of n in $\{p \in H_m : p_2 = n_2\}$. Thus, $n_1 < u_1 \leq n_1 + (a+1) \sum_{k=3}^{m} (i_k - j_k + 1)$. Now, let

$$w := (w_1, (i_2 - j_2)(a+1) + j_2, (i_3 - j_3)(a+1) + j_2, \ldots, (i_m - j_m)(a+1) + j_2),$$

where

$$w_1 = \max\left\{0, u_1 - (a+1)\sum_{k=3}^{m}(i_k - j_k + 1)\right\},$$

and let

$$h = \frac{\prod_{b\in\mathcal{B}\setminus\{b_2,\ldots,b_m\}}(y-b)}{\prod_{k=2}^{m}(y-b_k)^{i_k-j_k}x^{j_2}}.$$

Then $(h)_\infty = w_1 P_\infty + \sum_{k=2}^{m} w_k P_{0b_k}$. Thus, $w \in H_m$ and $w \preceq n$. Hence,

$$w = n.$$

As a result $w_1 = u_1 - (a+1)\sum_{k=3}^{m}(i_k - j_k + 1) > 0$ and $j_l = j_2$ for all $3 \le l \le m$. Moreover,

$$i_2 + \sum_{k=3}^{m}(i_k - j_k) + (m-2) = i_1 \text{ and } j_2 = j_1$$

by the uniqueness of representation of elements of the gap sets $G(P_\infty)$ and $G(P_{0b})$. Therefore,

$$n = \gamma_{j_2,(i_2-j_2+1,i_3-j_3+1,\ldots,i_m-j_m+1)}.$$

Finally, we must check that $\gamma_{j_2,(i_2-j_2+1,i_3-j_3+1,\ldots,i_m-j_m+1)} \in \Gamma_m$. To do this, we check that $\gamma_{j_2,(i_2-j_2+1,i_3-j_3+1,\ldots,i_m-j_m+1)} \in S_m$. Note that

$$\sum_{k=2}^{m}(i_k - j_k + 1) = i_1 - j_2 + 1,$$

$$1 \le j_2 = j_1 \le i_1 \le a - s, \text{ and}$$

which means

$$(s-1)(q-1) \le i_1 - j_2 \le s(q-1) - 1$$

where $1 \le s \le a + 1 - q^{r-1}$. Therefore, $\Gamma_m \subseteq S_m$. Thus, $\Gamma_m = S_m$ proving the desired

description of $\Gamma(P_\infty, P_{0b_2}, \ldots, P_{0b_m})$. $\square$

4.3 Examples

In this section, we consider two examples.

Example 11. Consider the norm-trace function field F/F_{q^r} with $r = 2$. Then $a = q$ and $F/\mathbb{F}_{q^2}$ is the Hermitian function field which has defining equation

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

Taking $m = 2$ in Theorem 28 gives the minimal generating set of $\Gamma(P_\infty, P_{0b_2})$. Because the automorphism group of F is doubly-transitive,

$$\Gamma(P_1, P_2) = \Gamma(P_\infty, P_{0b_2})$$

for any pair (P_1, P_2) of distinct degree one places of the Hermitian function field. This result first appeared as [25, Theorem 3.4].

More generally, the minimal generating set of the Weierstrass semigroup of the m-tuple $(P_\infty, P_{0b_2}, \ldots, P_{0b_m})$ of places of degree one of the Hermitian function field over $\mathbb{F}_{q^2}$ is

$$\Gamma_m = \left\{ \gamma_{j,\mathbf{t}} : \begin{array}{l} \sum_{k=2}^{m} t_k = i - j + 1, t_i \in \mathbb{Z}_+, 1 \leq j < i \leq q-1, \\ 0 \leq i - j \leq q - 2 \end{array} \right\}$$

where

$$\gamma_{j,\mathbf{t}} = \left(\left(q - \sum_{i=k}^{m} t_k \right)(q+1) - jq, (t_2 - 1)(q+1) + j, \ldots, (t_m - 1)(q+1) + j \right).$$

This result first appeared as [27, Theorem 10]. We also note that [24] contains some results

related to m-tuples on the Hermitian function field.

Example 12. Let $\mathbb{F}_{27} = \mathbb{F}_3(\omega)$ where $\omega^3 - \omega + 1 = 0$. The norm-trace function field with $q = 3$ and $r = 3$ is $\mathbb{F}_{27}(x, y)/\mathbb{F}_{27}$ where

$$y^9 + y^3 + y - x^{13}.$$

The genus of $\mathbb{F}_{27}(x, y)/\mathbb{F}_{27}$ is 48, and there are exactly 9 places of $\mathbb{F}_{27}(x, y)/\mathbb{F}_{27}$ of the form P_{0b}:

$$P_{00}, P_{01}, P_{02}, P_{0\omega}, P_{0\omega^3}, P_{0\omega^9}, P_{0\omega^{14}}, P_{0\omega^{16}}, P_{0\omega^{22}}.$$

Then

$$G(P_\infty) = \left\{ \begin{array}{l} 1, 2, 3, 4, 5, 6, 7, 8, 10, 11, 12, 14, 15, 16, 17, 19, 20, 21, 23, 24, 25, 28, \\ 29, 30, 32, 33, 34, 37, 38, 41, 42, 43, 46, 47, 50, 51, 55, 56, 59, 60, 64, \\ 68, 69, 73, 77, 82, 86, 95 \end{array} \right\},$$

and for all m, $2 \leq m \leq 10$,

$$G(P_{0b_m}) = \left\{ \begin{array}{l} 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 27, \\ 28, 29, 30, 31, 32, 33, 34, 40, 41, 42, 43, 44, 45, 46, 53, 54, 55, 56, 57, \\ 66, 67, 68, 69, 79, 80, 92 \end{array} \right\}.$$

Taking $m = 2$ in Theorem 28 yields $\Gamma\left(P_\infty, P_{0b_2}\right) =$

$$\left\{\begin{array}{l}(1,23),(2,46),(3,69),(4,92),(5,11),(6,34),(7,57),(8,80),(10,22),\\(11,45),(12,68),(14,10),(15,33),(16,56),(17,79),(19,21),(20,44),\\(21,67),(23,9),(24,32),(25,55),(28,20),(29,43),(30,66),(32,8),(33,31),\\(34,54),(37,19),(38,42),(41,7),(42,30),(43,53),(46,18),(47,41),(50,6),\\(51,29),(55,17),(56,40),(59,5),(60,28),(64,16),(68,4),(69,27),\\(73,15),(77,3),(82,14),(86,2),(95,1)\end{array}\right\};$$

this also follows from Lemma 27. Figure 4.1 illustrates how the minimal generating set $\Gamma\left(P_\infty, P_{0b_2}\right)$ is related to the semigroup $H\left(P_\infty, P_{0b_2}\right)$. In particular, the elements of $\Gamma\left(P_\infty, P_{0b_2}\right)$ are shown in bold as are the elements of $\Gamma\left(P_\infty\right) \cap [0, 2g]$ and $\Gamma\left(P_{0b_2}\right) \cap [0, 2g]$.

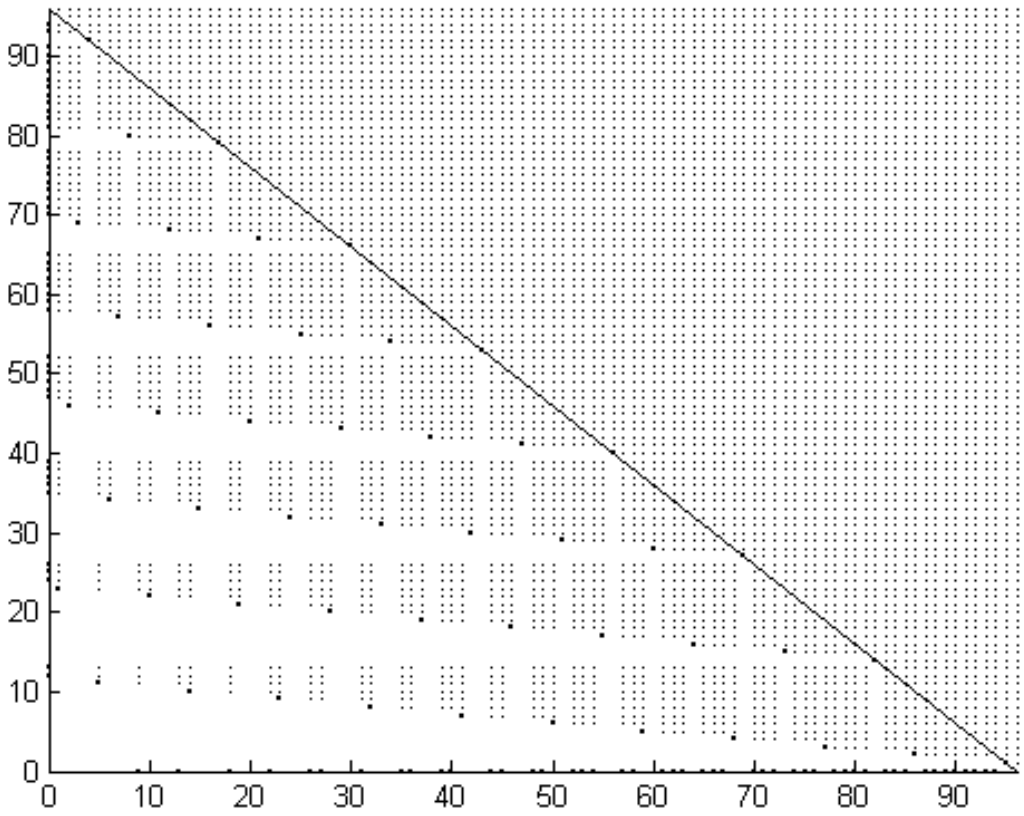


Figure 4.1: $H\left(P_{\infty}, P_{0b_2}\right) \cap [0, 2g]^2$

Taking $m = 3$ in Theorem 28 gives $\Gamma\left(P_\infty, P_{0b_2}, P_{0b_3}\right) =$

$$\left\{\begin{array}{l}
(1,10,10),(2,7,33),(2,20,20),(2,33,7),(3,4,56),(3,17,43),\\
(3,30,30),(3,43,17),(3,56,4),(4,1,79),(4,14,66),(4,27,53),\\
(4,40,40),(4,53,27),(4,66,14),(4,79,1),(6,8,21),(6,21,8),\\
(7,5,44),(7,18,31),(7,31,18),(7,44,5),(8,2,67),(8,15,54),\\
(8,28,41),(8,41,28),(8,54,15),(8,67,2),(10,9,9),(11,6,32),\\
(11,19,19),(11,32,6),(12,3,55),(12,16,42),(12,29,29),(12,42,16),\\
(12,55,3),(15,7,20),(15,20,7),(16,4,43),(16,17,30),(16,30,17),\\
(16,43,4),(17,1,66),(17,14,53),(17,27,40),(17,40,27),(17,53,14),\\
(17,66,1),(19,8,8),(20,5,31),(20,18,18),(20,31,5),(21,2,54),\\
(21,15,41),(21,28,28),(21,41,15),(21,54,2),(24,6,19),(24,19,6),\\
(25,3,42),(25,16,29),(25,29,16),(25,42,3),(28,7,7),(29,4,30),\\
(29,17,17),(29,30,4),(30,1,53),(30,14,40),(30,27,27),(30,40,14),\\
(30,53,1),(33,5,18),(33,18,5),(34,2,41),(34,15,28),(34,28,15),\\
(34,41,2),(37,6,6),(38,3,29),(38,16,16),(38,29,3),(42,4,17),\\
(42,17,4),(43,1,40),(43,14,27),(43,27,14),(43,40,1),(46,5,5),\\
(47,2,28),(47,15,15),(47,28,2),(51,3,16),(51,16,3),(55,4,4),\\
(56,1,27),(56,14,14),(56,27,1),(60,2,15),(60,15,2),(64,3,3),\\
(69,1,14),(69,14,1),(73,2,2),(82,1,1)
\end{array}\right\},$$

as shown in [29].

Considering $4 \leq m \leq 10$ in Theorem 28 gives $\Gamma\left(P_{\infty}, P_{0b_2}, P_{0b_3}, P_{0b_4}\right) =$

$$\left\{\begin{array}{l}
(69,1,1,1),(56,1,1,14),(56,1,14,1),(56,14,1,1),(60,2,2,2),(47,2,2,15), \\
(47,2,15,2),(47,15,2,2),(51,3,3,3),(38,3,3,16),(38,3,16,3),(38,16,3,3), \\
(42,4,4,4),(29,4,4,17),(29,4,17,4),(29,17,4,4),(33,5,5,5),(20,5,5,18), \\
(20,5,18,5),(20,18,5,5),(24,6,6,6),(11,6,6,19),(11,6,19,6),(11,19,6,6), \\
(15,7,7,7),(2,7,7,20),(2,7,20,7),(2,20,7,7),(6,8,8,8),(43,1,1,27), \\
(43,1,14,14),(43,1,27,1),(43,14,1,14),(43,14,14,1),(43,27,1,1),(30,1,1,40), \\
(30,1,14,27),(30,1,27,14),(30,1,40,1),(30,14,1,27),(30,14,14,14),(30,14,27,1), \\
(30,27,1,14),(30,27,14,1),(30,40,1,1),(34,2,2,28),(34,2,15,15),(34,2,28,2), \\
(34,15,2,15),(34,15,15,2),(34,28,2,2),(21,2,2,41),(21,2,15,28),(21,2,28,15), \\
(21,2,41,2),(21,15,2,28),(21,15,15,15),(21,15,28,2),(21,28,2,15),(21,28,15,2), \\
(21,41,2,2),(25,3,3,29),(25,3,16,16),(25,3,29,3),(25,16,3,16),(25,16,16,3), \\
(25,29,3,3),(12,3,3,42),(12,3,16,29),(12,3,29,16),(12,3,42,3),(12,16,3,29), \\
(12,16,16,16),(12,16,29,3),(12,29,3,16),(12,29,16,3),(12,42,3,3),(16,4,4,30), \\
(16,4,17,17),(16,4,30,4),(16,17,4,17),(16,17,17,4),(16,30,4,4),(3,4,4,43), \\
(3,4,17,30),(3,4,30,17),(3,4,43,4),(3,17,4,30),(3,17,17,17),(3,17,30,4), \\
(3,30,4,17),(3,30,17,4),(3,43,4,4),(7,5,5,31),(7,5,18,18),(7,5,31,5), \\
(7,18,5,18),(7,18,18,5),(7,31,5,5),(17,1,1,53),(17,1,14,40),(17,1,27,27), \\
(17,1,40,14),(17,1,53,1),(17,14,1,40),(17,14,14,27),(17,14,27,14),(17,14,40,1), \\
(17,27,1,27),(17,27,14,14),(17,27,27,1),(17,40,1,14),(17,40,14,1),(17,53,1,1), \\
(4,1,1,66),(4,1,14,53),(4,1,27,40),(4,1,40,27),(4,1,53,14),(4,1,66,1), \\
(4,14,1,53),(4,14,14,40),(4,14,27,27),(4,14,40,14),(4,14,53,1),(4,27,1,40), \\
(4,27,14,27),(4,27,27,14),(4,27,40,1),(4,40,1,27),(4,40,14,14),(4,40,27,1), \\
(4,53,1,14),(4,53,14,1),(4,66,1,1),(8,2,2,54),(8,2,15,41),(8,2,28,28), \\
(8,2,41,15),(8,2,54,2),(8,15,2,41),(8,15,15,28),(8,15,28,15),(8,15,41,2), \\
(8,28,2,28),(8,28,15,15),(8,28,28,2),(8,41,2,15),(8,41,15,2),(8,54,2,2)
\end{array}\right\},$$

$\Gamma\left(P_{\infty}, P_{0b_2}, P_{0b_3}, P_{0b_4}, P_{0b_5}\right) =$

$$\left\{\begin{array}{l}
(56,1,1,1,1),(47,2,2,2,2),(38,3,3,3,3),(29,4,4,4,4),(20,5,5,5,5),(11,6,6,6,6),\\
(2,7,7,7,7),(43,1,1,1,14),(43,1,1,14,1),(43,1,14,1,1),(43,14,1,1,1),(30,1,1,1,27),\\
(30,1,1,14,14),(30,1,1,27,1),(30,1,14,1,14),(30,1,14,14,1),(30,1,27,1,1),\\
(30,14,1,1,14),(30,14,1,14,1),(30,14,14,1,1),(30,27,1,1,1),(34,2,2,2,15),\\
(34,2,2,15,2),(34,2,15,2,2),(34,15,2,2,2),(21,2,2,2,28),(21,2,2,15,15),\\
(21,2,2,28,2),(21,2,15,2,15),(21,2,15,15,2),(21,2,28,2,2),(21,15,2,2,15),\\
(21,15,2,15,2),(21,15,15,2,2),(21,28,2,2,2),(25,3,3,3,16),(25,3,3,16,3),\\
(25,3,16,3,3),(25,16,3,3,3),(12,3,3,3,29),(12,3,3,16,16),(12,3,3,29,3),\\
(12,3,16,3,16),(12,3,16,16,3),(12,3,29,3,3),(12,16,3,3,16),(12,16,3,16,3),\\
(12,16,16,3,3),(12,29,3,3,3),(16,4,4,4,17),(16,4,4,17,4),(16,4,17,4,4),(16,17,4,4,4),\\
(3,4,4,4,30),(3,4,4,17,17),(3,4,4,30,4),(3,4,17,4,17),(3,4,17,17,4),\\
(3,4,30,4,4),(3,17,4,4,17),(3,17,4,17,4),(3,17,17,4,4),(3,30,4,4,4),\\
(7,5,5,5,18),(7,5,5,18,5),(7,5,18,5,5),(7,18,5,5,5),(17,1,1,1,40),(17,1,1,14,27),\\
(17,1,1,27,14),(17,1,1,40,1),(17,1,14,1,27),(17,1,14,14,14),(17,1,14,27,1),\\
(17,1,27,1,14),(17,1,27,14,1),(17,1,40,1,1),(17,14,1,1,27),(17,14,1,14,14),\\
(17,14,1,27,1),(17,14,14,1,14),(17,14,14,14,1),(17,14,27,1,1),(17,27,1,1,14),\\
(17,27,1,14,1),(17,27,14,1,1),(17,40,1,1,1),(4,1,1,1,53),(4,1,1,14,40),(4,1,1,27,27),\\
(4,1,1,40,14),(4,1,1,53,1),(4,1,14,1,40),(4,1,14,14,27),(4,1,14,27,14),(4,1,14,40,1),\\
(4,1,27,1,27),(4,1,27,14,14),(4,1,27,27,1),(4,1,40,1,14),(4,1,40,14,1),\\
(4,1,53,1,1),(4,14,1,1,40),(4,14,1,14,27),(4,14,1,27,14),(4,14,1,40,1),\\
(4,14,14,1,27),(4,14,14,14,14),(4,14,14,27,1),(4,14,27,1,14),(4,14,27,14,1),\\
(4,14,40,1,1),(4,27,1,1,27),(4,27,1,14,14),(4,27,1,27,1),(4,27,14,1,14),\\
(4,27,14,14,1),(4,27,27,1,1),(4,40,1,1,14),(4,40,1,14,1),(4,40,14,1,1),\\
(4,53,1,1,1),(8,2,2,2,41),(8,2,2,15,28),(8,2,2,28,15),(8,2,2,41,2),(8,2,15,2,28),\\
(8,2,15,15,15),(8,2,15,28,2),(8,2,28,2,15),(8,2,28,15,2),(8,2,41,2,2),\\
(8,15,2,2,28),(8,15,2,15,15),(8,15,2,28,2),(8,15,15,2,15),(8,15,15,15,2),\\
(8,15,28,2,2),(8,28,2,2,15),(8,28,2,15,2),(8,28,15,2,2),(8,41,2,2,2)
\end{array}\right\},$$

$\Gamma\left(P_{\infty}, P_{0b_2}, P_{0b_3}, P_{0b_4}, P_{0b_5}, P_{0b_6}\right) =$

$$\left\{\begin{array}{l}
(43,1,1,1,1,1),(30,1,1,1,1,14),(30,1,1,1,14,1),(30,1,1,14,1,1),\\
(30,1,14,1,1,1),(30,14,1,1,1,1),(34,2,2,2,2,2),(21,2,2,2,2,15),\\
(21,2,2,2,15,2),(21,2,2,15,2,2),(21,2,15,2,2,2),(21,15,2,2,2,2),\\
(25,3,3,3,3,3),(12,3,3,3,3,16),(12,3,3,3,16,3),(12,3,3,16,3,3),\\
(12,3,16,3,3,3),(12,16,3,3,3,3),(16,4,4,4,4,4),(3,4,4,4,4,17),\\
(3,4,4,4,17,4),(3,4,4,17,4,4),(3,4,17,4,4,4),(3,17,4,4,4,4),\\
(7,5,5,5,5,5),(17,1,1,1,1,27),(17,1,1,1,14,14),(17,1,1,1,27,1),\\
(17,1,1,14,1,14),(17,1,1,14,14,1),(17,1,1,27,1,1),(17,1,14,1,1,14),\\
(17,1,14,1,14,1),(17,1,14,14,1,1),(17,1,27,1,1,1),(17,14,1,1,1,14),\\
(17,14,1,1,14,1),(17,14,1,14,1,1),(17,14,14,1,1,1),(17,27,1,1,1,1),\\
(4,1,1,1,1,40),(4,1,1,1,14,27),(4,1,1,1,27,14),(4,1,1,1,40,1),\\
(4,1,1,14,1,27),(4,1,1,14,14,14),(4,1,1,14,27,1),(4,1,1,27,1,14),\\
(4,1,1,27,14,1),(4,1,1,40,1,1),(4,1,14,1,1,27),(4,1,14,1,14,14),\\
(4,1,14,1,27,1),(4,1,14,14,1,14),(4,1,14,14,14,1),(4,1,14,27,1,1),\\
(4,1,27,1,1,14),(4,1,27,1,14,1),(4,1,27,14,1,1),(4,1,40,1,1,1),\\
(4,14,1,1,1,27),(4,14,1,1,14,14),(4,14,1,1,27,1),(4,14,1,14,1,14),\\
(4,14,1,14,14,1),(4,14,1,27,1,1),(4,14,14,1,1,14),(4,14,14,1,14,1),\\
(4,14,14,14,1,1),(4,14,27,1,1,1),(4,27,1,1,1,14),(4,27,1,1,14,1),\\
(4,27,1,14,1,1),(4,27,14,1,1,1),(4,40,1,1,1,1),(8,2,2,2,2,28),\\
(8,2,2,2,15,15),(8,2,2,2,28,2),(8,2,2,15,2,15),(8,2,2,15,15,2),\\
(8,2,2,28,2,2),(8,2,15,2,2,15),(8,2,15,2,15,2),(8,2,15,15,2,2),\\
(8,2,28,2,2,2),(8,15,2,2,2,15),(8,15,2,2,15,2),(8,15,2,15,2,2),\\
(8,15,15,2,2,2),(8,28,2,2,2,2)
\end{array}\right\},$$

$\Gamma\left(P_{\infty}, P_{0b_2}, P_{0b_3}, P_{0b_4}, P_{0b_5}, P_{0b_6}, P_{0b_7}\right) =$

$$\left\{\begin{array}{l}(30,1,1,1,1,1,1),(21,2,2,2,2,2,2),(12,3,3,3,3,3,3),\\(3,4,4,4,4,4,4),(17,1,1,1,1,1,14),(17,1,1,1,1,14,1),\\(17,1,1,1,14,1,1),(17,1,1,14,1,1,1),(17,1,14,1,1,1,1),\\(17,14,1,1,1,1,1),(4,1,1,1,1,1,27),(4,1,1,1,1,14,14),\\(4,1,1,1,1,27,1),(4,1,1,1,14,1,14),(4,1,1,1,14,14,1),\\(4,1,1,1,27,1,1),(4,1,1,14,1,1,14),(4,1,1,14,1,14,1),\\(4,1,1,14,14,1,1),(4,1,1,27,1,1,1),(4,1,14,1,1,1,14),\\(4,1,14,1,1,14,1),(4,1,14,1,14,1,1),(4,1,14,14,1,1,1),\\(4,1,27,1,1,1,1),(4,14,1,1,1,1,14),(4,14,1,1,1,14,1),\\(4,14,1,1,14,1,1),(4,14,1,14,1,1,1),(4,14,14,1,1,1,1),\\(4,27,1,1,1,1,1),(8,2,2,2,2,2,15),(8,2,2,2,2,15,2),\\(8,2,2,2,15,2,2),(8,2,2,15,2,2,2),(8,2,15,2,2,2,2),\\(8,15,2,2,2,2,2)\end{array}\right\},$$

$\Gamma\left(P_{\infty}, P_{0b_2}, P_{0b_3}, P_{0b_4}, P_{0b_5}, P_{0b_6}, P_{0b_7}, P_{0b_8}\right) =$

$$\left\{\begin{array}{l}(17,1,1,1,1,1,1,1),(4,1,1,1,1,1,1,14),(4,1,1,1,1,1,14,1),\\(4,1,1,1,1,14,1,1),(4,1,1,1,14,1,1,1),(4,1,1,14,1,1,1,1),\\(4,1,14,1,1,1,1,1),(4,14,1,1,1,1,1,1),(8,2,2,2,2,2,2,2)\end{array}\right\},$$

$\Gamma\left(P_{\infty}, P_{0b_2}, P_{0b_3}, P_{0b_4}, P_{0b_5}, P_{0b_6}, P_{0b_7}, P_{0b_8}, P_{0b_9}\right) =$

$$\left\{\begin{array}{l}(4,1,1,1,1,1,1,1,1)\end{array}\right\},$$

and

$$\Gamma\left(P_{\infty}, P_{0b_2}, P_{0b_3}, P_{0b_4}, P_{0b_5}, P_{0b_6}, P_{0b_7}, P_{0b_8}, P_{0b_9}, P_{0b_{10}}\right) = \emptyset.$$

4.4 Minimal generating sets of m-tuples not containing P_∞

Next, we use Corollary 10 and Lemma 26 to find minimal generating sets of the Weierstrass semigroups $H(P_{0\beta_1}, \ldots, P_{0\beta_m})$ on the norm-trace function field. Recall that the gap set of any place $P_{0\beta}$ where $\beta \in \mathcal{B}$ is

$$G(P_{0\beta}) = \left\{ (i-j)(a+1)+j : \begin{array}{c} 1 \leq j \leq i \leq a-s \text{ and} \\ (s-1)(q-1) \leq i-j < s(q-1) \\ \text{where } 1 \leq s \leq a+1-q^{r-1} \end{array} \right\}.$$

Theorem 29. *Let $2 \leq m \leq q^{r-1}$. The minimal generating set of the Weierstrass semigroup $H(P_{0\beta_1}, \ldots, P_{0\beta_m})$ of the norm-trace function field over $\mathbb{F}_{q^r}$ is $\Gamma(P_{0\beta_1}, \ldots, P_{0\beta_m}) =$*

$$\left\{ (t_1(a+1)+j, \ldots, t_m(a+1)+j) : \begin{array}{l} 1 \leq j \leq a-1, t_i \in \mathbb{N}, \\ \sum_{i=1}^m t_i = q^{r-1} + \left\lfloor \frac{j-1}{q} \right\rfloor - m - j + 1 \end{array} \right\}.$$

Proof. First, we show that $T \subseteq \Gamma(P_{0\beta_1}, \ldots, P_{0\beta_m})$ where

$$T = \left\{ (t_1(a+1)+j, \ldots, t_m(a+1)+j) : \begin{array}{l} 1 \leq j \leq a-1, t_i \in \mathbb{N}, \\ \sum_{i=1}^m t_i = q^{r-1} + \left\lfloor \frac{j-1}{q} \right\rfloor - m - j + 1 \end{array} \right\}.$$

Let

$$\alpha := (t_1(a+1)+j, \ldots, t_m(a+1)+j) \in T.$$

Then $\alpha \in H(P_{0\beta_1}, \ldots, P_{0\beta_m})$ as

$$\left(\frac{x^{a+1-j}}{\prod_{i=1}^m (y-\beta_i)^{t_i+1}} \right)_\infty = \sum_{i=1}^m (t_i(a+1)+j) P_{0\beta_i};$$

here, it is helpful to note that

$$\begin{aligned} v_{P_\infty}\left(\tfrac{x^{a+1-j}}{\prod_{i=1}^{m}(y-\beta_i)^{t_i+1}}\right) &= (a+1)\left(\textstyle\sum_{i=1}^{m} t_i + m - q^{r-1}\right) + jq^{r-1} \\ &= (a+1)\left(\left\lfloor \tfrac{j-1}{q} \right\rfloor - j + 1\right) + jq^{r-1} \\ &= (a+1)\left(1 - \tfrac{j-1 \mod q+1}{q}\right) + \tfrac{j}{q} > 0. \end{aligned}$$

It remains to prove that

$$\ell\left(\sum_{i=1}^{m}(\alpha_i - 1)\,P_{0\beta_i}\right) = \ell\left((\alpha_i - 1)\,P_{0\beta_i} + \sum_{\substack{k=1 \\ k\neq i}}^{m} \alpha_k P_{0\beta_k}\right) \tag{4.2}$$

for all i, $1 \le i \le m$. According to Corollary 2.2,

$$\ell\left(\sum_{i=1}^{m}(\alpha_i - 1)\,P_{0\beta_i}\right) = \sum_{i=0}^{a}\max\{C_i, 0\}$$

and

$$\ell\left((\alpha_1 - 1)\,P_{0\beta_1} + \sum_{i=2}^{m}\alpha_i P_{0\beta_i}\right) = \sum_{i=0}^{a}\max\{D_i, 0\}$$

where $C_i = \left\lfloor \frac{-iq^{r-1}}{a+1} \right\rfloor + \sum_{k=1}^{m}\left\lfloor \frac{\alpha_k - 1 + i}{a+1} \right\rfloor + 1$ and

$$D_i = \left\lfloor \frac{-iq^{r-1}}{a+1} \right\rfloor + \left\lfloor \frac{\alpha_1 - 1 + i}{a+1} \right\rfloor + \sum_{k=2}^{m}\left\lfloor \frac{\alpha_k + i}{a+1} \right\rfloor + 1.$$

Clearly, $C_i \le D_i$ for all i, $0 \le i \le a$. In fact, $C_i = D_i$ unless $i = a + 1 - k$. However,

$$D_{a+1-k} = \left\lfloor \frac{kq^{r-1}}{a+1} \right\rfloor + \left\lfloor \frac{k-1}{q} \right\rfloor - k + 1 \le \left\lfloor \frac{kq^{r-1}}{a+1} + \frac{k-1}{q} \right\rfloor - k + 1 \le 0.$$

As a result,

$$\sum_{i=0}^{a} \max\{C_i, 0\} = \sum_{i=0}^{a} \max\{D_i, 0\},$$

and $\ell\left(\sum_{i=1}^{m}(\alpha_i - 1)P_{0\beta_i}\right) = \ell\left((\alpha_1 - 1)P_{0\beta_1} + \sum_{i=2}^{m}\alpha_i P_{0\beta_i}\right)$. Hence, Equation (4.2) holds for $i = 1$. The cases $2 \leq i \leq m$ follow from a simlar argument; thus, $\alpha \in \Gamma(P_{0\beta_1}, \ldots, P_{0\beta_m})$. Therefore, $T \subseteq \Gamma(P_{0\beta_1}, \ldots, P_{0\beta_m})$.

Next, we prove that $\Gamma(P_{0\beta_1}, \ldots, P_{0\beta_m}) \subseteq T$. Suppose α is an element of $\Gamma(P_{0\beta_1}, \ldots, P_{0\beta_m})$. Then

$$\alpha = (t_1(a+1) + j_1, \ldots, t_m(a+1) + j_m) \in G(P_{0\beta_1}) \times G(P_{0\beta_m})$$

where for each k, $1 \leq k \leq m$, $t_k \in \mathbb{N}$ and $1 \leq j_k \leq a - 1$, and by Lemma 26,

$$\ell\left(\sum_{k=1}^{m}\alpha_k P_{0\beta_k}\right) = \ell\left(\sum_{k=1}^{m}(\alpha_k - 1)P_{0\beta_k}\right) + 1.$$

Applying Corollary 2.2 gives

$$\sum_{i=0}^{a} \max\{A_i, 0\} = \sum_{i=0}^{a} \max\{B_i, 0\} + 1$$

where

$$A_i = \left\lfloor \frac{-iq^{r-1}}{a+1} \right\rfloor + \sum_{k=1}^{m} t_k + \sum_{k=1}^{m} \left\lfloor \frac{j_k + i}{a+1} \right\rfloor + 1$$

and

$$B_i = \left\lfloor \frac{-iq^{r-1}}{a+1} \right\rfloor + \sum_{k=1}^{m} t_k + \sum_{k=1}^{m} \left\lfloor \frac{j_k + i - 1}{a+1} \right\rfloor + 1.$$

Consequently, there exists $j \in \{j_k : 1 \leq k \leq m\}$ such that $i = a + 1 - j$ and

$$A_i = \max\{A_i, 0\} = \max\{B_i, 0\} + 1;$$

for $i \neq a+1-j$, $\max\{A_i, 0\} = \max\{B_i, 0\}$. It follows that $A_{a+1-j} \geq 1$. This implies

$$\sum_{k=1}^{m} t_k \geq q^{r-1} - \left\lfloor \frac{jq^{r-1}}{a+1} \right\rfloor - (\#j_k \geq j) = q^{r-1} - j + \left\lfloor \frac{j-1}{q} \right\rfloor + 1 - (\#j_k \geq j).$$

Now define $u = (T_1(a+1)+j, \ldots, T_m(a+1)+j)$ where

$$T_k = \begin{cases} t_k & \text{if } j \leq j_k \\ t_k - 1 & \text{if } j > j_k. \end{cases}$$

Then $u \preceq \alpha$. By the argument above, there exists

$$s := (s_1(a+1)+j, \ldots, s_m(a+1)+j) \in T \subseteq H(P_{0\beta_1}, \ldots, P_{0\beta_m})$$

where $\sum_{k=1}^{m} s_k = q^{r-1} + \left\lfloor \frac{j-1}{q} \right\rfloor - j - m + 1$ and $s_k \leq T_k$ for all k, $1 \leq k \leq m$. Hence, there exists $h \in F$ with $(h)_\infty = \sum_{k=1}^{m} s_k P_{0\beta_k}$. Then $u \in H(P_{0\beta_1}, \ldots, P_{0\beta_m})$ follows from considering $\frac{h}{\prod_{k=1}^{m}(y-\beta_k)^{T_k - s_k}}$. Therefore, $\alpha = u$. It follows that $j_1 = \cdots = j_m = j$ and $\sum_{k=1}^{m} t_k \geq q^{r-1} + \left\lfloor \frac{j-1}{q} \right\rfloor - j - m + 1$. Then $\sum_{k=1}^{m} t_k = q^{r-1} + \left\lfloor \frac{j-1}{q} \right\rfloor - j - m + 1$ as otherwise, there exists an element of T which is less than α. Therefore, $\alpha \in T$. $\square$

The next example demonstrates the use of Theorem 29 and the relationship between the Weierstrass semigroup $H(P_1, \ldots, P_m)$ and its minimal generating set $\Gamma(P_1, \ldots, P_m)$.

Example 13. *Consider the norm-trace function field $\mathbb{F}_{27}(x,y)/\mathbb{F}_{27}$ where*

$$y^9 + y^3 + y = x^{13},$$

$\mathbb{F}_{27} := \mathbb{F}_3(\omega)$ and $\omega^3 + 2\omega + 1 = 0$. The genus of this function field is $g = 48$ Here, $q = 3$,

$r = 3$, and $u = 12$. Then Theorem 29 yields

$$\Gamma\left(P_{0\beta_1}, P_{0\beta_2}\right) = \left\{ \begin{array}{l} (1,92), (2,80), (3,68), (4,69), (5,57), (6,45), (7,46), \\ (8,34), (9,22), (10,23), (11,11), (14,79), (15,67), \\ (16,55), (17,56), (18,44), (19,32), (20,33), (21,21), \\ (22,9), (23,10), (27,66), (28,54), (29,42), (30,43), \\ (31,31), (32,19), (33,20), (34,8), (40,53), (41,41), \\ (42,29), (43,30), (44,18), (45,6), (46,7), (53,40), \\ (54,28), (55,16), (56,17), (57,5), (66,27), (67,15), \\ (68,3), (69,4), (79,14), (80,2), (92,1) \end{array} \right\}$$

for any distinct $\beta_1, \beta_2 \in \mathcal{B} = \{0, 1, 2, \omega, \omega^3, \omega^9, \omega^{14}, \omega^{16}, \omega^{22}\}$.

Figure 4.2 at the end of this section illustrates the relationship between the minimal generating set $\Gamma\left(P_{0\beta_1}, P_{0\beta_2}\right)$ and the Weierstrass semigroup $H\left(P_{0\beta_1}, P_{0\beta_2}\right)$. In particular, the elements of $\Gamma\left(P_{0\beta_1}, P_{0\beta_2}\right)$ are shown in red as are the elements of $\left(\Gamma\left(P_{0\beta_1}\right) \cap [0, 2g]\right) \times \{0\}$ and $\{0\} \times \left(\Gamma\left(P_{0\beta_2}\right) \cap [0, 2g]\right)$. The remaining elements of $H\left(P_{0\beta_1}, P_{0\beta_2}\right)$ are those generated by the least upper bound operation; those in the region $[0, 2g]^2$ are shown in black. The line segment in Figure 4.2 is given by $x + y = 2g$. All pairs (x, y) with $x + y \geq 2g$, meaning those above or to the right of this line segment, are elements of $H\left(P_{0\beta_1}, P_{0\beta_2}\right)$ according to the Riemann-Roch Theorem.

The Weierstrass semigroups $H\left(P_\infty, P_{0b_2}, \ldots, P_{0b_m}\right)$, $m \geq 3$, are also a consequence of Theorem 29. In the previous section, the minimal generating set $\Gamma\left(P_\infty, P_{0b_2}, \ldots, P_{0b_m}\right)$ is shown to be

$$\left\{ \gamma_{j,\mathbf{t}} : \begin{array}{l} \sum_{k=2}^{m} t_k = i - j + 1, t_k \in \mathbb{Z}_+, 1 \leq j \leq i \leq a - s, \\ (s-1)(q-1) \leq i - j \leq s(q-1) - 1 \\ \text{where } 1 \leq s \leq a + 1 - q^{r-1} \end{array} \right\}$$

where $2 \leq m \leq q^{r-1}+1$ and

$$\gamma_{j,\mathbf{t}} = \left(\left(q^{r-1} - \sum_{k=2}^{m} t_k \right) (a+1) - jq^{r-1}, (t_2-1)(a+1)+j, \ldots, (t_m-1)(a+1)+j \right).$$

However, this alone does not determine $H\left(P_\infty, P_{0b_2}, \ldots, P_{0b_m}\right)$ for $m \geq 3$ as one must also know $\Gamma\left(P_{0b_1}, \ldots, P_{0b_m}\right)$ for $1 \leq m \leq q^{r-1}$. This is now provided via Theorem 29.

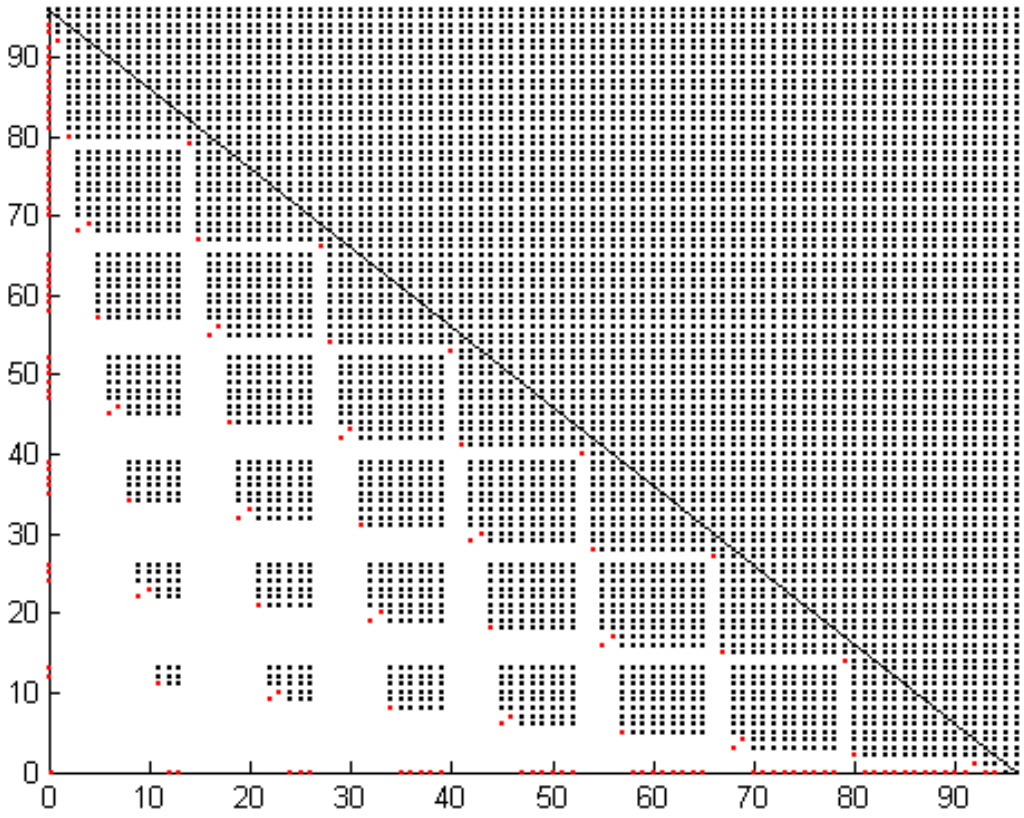


Figure 4.2: $H\left(P_{0b_1}, P_{0b_2}\right) \cap [0, 2g]^2$

Chapter 5

Weierstrass semigroups arising from a finite graph

In [4], Baker and Norine developed a Riemann-Roch theory for a finite connected graph G containing no loops. In [3], Baker further explored this theory and defined a Weierstrass gap. We apply the construction given in [4] to construct a second analogue of Weierstass semigroups. This chapter is organized as follows. Section 2 includes a overview of the Riemann-Roch theory on a finite graph. Section 3 contains the main results.

Notation. Given $a_1, \ldots, a_k \in \mathbb{Z}^+$, the (numerical) semigroup generated by $a_1, \ldots, a_k$ is

$$\langle a_1, \ldots, a_k \rangle := \left\{ \sum_{i=1}^{k} c_i a_i : c_i \in \mathbb{N} \right\}.$$

All graphs in this chapter are finite, connected, and without loops. Hence, we say a graph to mean a graph satisfying these conditions.

5.1 Riemann-Roch on finite graphs

In this section, we follow the construction given by Baker and Norine in [4]. Let $V(G) = \{P_1, P_2, \ldots, P_n\}$ be the set of vertices of a graph G. Let $Div(G)$ be the free abelian group on $\{P_1, P_2, \ldots, P_n\}$, the set of vertices of G. Then, a divisor D is an element of $Div(G)$, that is,

$$D = \sum_{i=1}^{n} a_i P_i,$$

where $a_i \in \mathbb{Z}$. A divisor D is effective if and only if $a_i \geq 0$ for all $P_i \in V(G)$, and the degree of D is defined to be $\sum_{i=1}^{n} a_i$. Then, we denote the subset of all effective divisors of degree k by $Div_+^k(G) = \{D \in Div(G) : D \geq 0 \text{ and } \deg(D) = k\}$.

Consider the abelian group of integer-valued functions on the vertices of G,

$$\mathcal{M}(G) = Hom\{V(G), \mathbb{Z}\}.$$

As in the function field setting, we would like to consider the divisor of $f \in \mathcal{M}(G)$. Let $Nbhd(v)$ denote the set of all vertices adjacent to v. If $f \in \mathcal{M}(G)$, the divisor $\Delta(f)$ is

$$\Delta(f) = \sum_{v \in V(G)} \Delta_v(f) v$$

where

$$\Delta_v(f) = \sum_{w \in Nbhd(v)} (f(v) - f(w)) \in \mathbb{Z}.$$

Let A be the adjacency matrix of the graph G, that is, $A \in \mathbb{Z}^{n \times n}$ where A_{ij} is the number of edges between P_i and P_j. Let D is the matrix defined so that $D_{ij} = 0$ if $i \neq j$ and

$D_{ii} = \deg(P_i)$. Then, the Laplacian of G is the matrix $Q = D - A$. Hence,

$$Q_{ij} = \begin{cases} -|\{\text{edges between } P_i \text{ and } P_j\}| & \text{if } i \neq j \\ \deg(P_i) & \text{if } i = j \end{cases}.$$

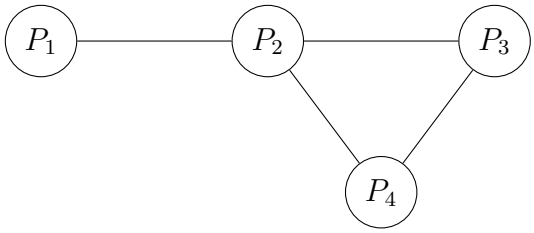
Let $(P_1, P_2, \ldots, P_n)$ be the ordered set of vertices of a graph G. Then, if $f \in \mathcal{M}(G)$, we define $[f] \in \mathbb{Z}^n$ by $[f]_i = f(P_i)$. Similarly, if $D \in Div(G)$ where $D = \sum_{i=1}^{n} a_i P_i$, $[D]_i = a_i$.Note that if Q is the Laplacian of G,

$$[\Delta(f)] = Q\,[f]\,.$$

Example 14. Consider the graph G given below. Then

$$\mathcal{M}(G) = \{f : f(P_i) \in \mathbb{Z} \text{ for } i = 1, 2, 3, 4\}.$$

Consider $f \in \mathcal{M}(G)$ such that $f(P_1) = -1$, $f(P_3) = -1$, $f(P_2) = 0$, and $f(P_4) = 0$.



Then,

- $\Delta_{P_1}(f) = -1 - 0$.
- $\Delta_{P_2}(f) = (0 - (-1)) + (0 - (-1))$.
- $\Delta_{P_3}(f) = (-1 - 0) + (-1 - 0)$.
- $\Delta_{P_4}(f) = 0 - (-1)$.

Thus, $\Delta(f) = 2P_2 + P_4 - P_1 - 2P_3$.

Thus we may view $\Delta(f)$ as an analogue of (f) and $\Delta_v(f)$ as an analogue of $v_P(f)$ in the function field case. We have the following result which follows from the rank of the Laplacian.

Proposition 30. *Let G be a graph and $f \in \mathcal{M}(G)$. Then,*

$$\deg(\Delta(f)) = 0.$$

Proof. Note that $\deg(\Delta(f)) = \sum_v \Delta_v(f) = \sum_v \sum_{w \in Nbhd(v)} (f(v) - f(w))$. Thus, it must be that $\deg(\Delta(f)) = \frac{1}{2} \sum_{\substack{v \in V(G) \\ w \in Nbhd(v)}} [(f(v) - f(w)) + (f(w) - f(v))] = 0$. □

Definition 25. The dimension of a divisor $D \in Div(G)$ is

$$r(D) = \max\left\{k : \text{ there exists } f \in \mathcal{M}(G) \text{ such that } \Delta(f) \geq E - D \text{ for all } E \in Div_+^k(G)\right\}.$$

As in the algebraic geometry setting, there exists a relationship between the dimension of a divisor and its degree. This is known as the Riemann-Roch Theorem for finite graphs.

Theorem 31. *[4] Let G be a graph, $D \in Div(G)$, $K = \sum_{v \in V(G)} (\deg(v) - 2)v$, and $g = |E(G)| - |V(G)| + 1$. Then,*

$$r(D) = \deg(D) + 1 - g + r(K - D).$$

5.2 Weierstrass semigroups on finite graphs

In this section we focus on two possible analogues of $H(P)$ in the case of a finite graph.

Definition 26. Let G be a graph and $P \in V(G)$. Then,

$$H_r(P) = \{\alpha \in \mathbb{N} \ : \ r(\alpha P) = r((\alpha - 1)P) + 1\}$$

and

$$H_f(P) = \left\{ \alpha \in \mathbb{N} : \begin{array}{c} \text{there exists } f \in \mathcal{M}(G) \text{ such that} \\ \Delta(f) = A - \alpha P \text{ where } A \geq 0 \text{ and } P \notin \text{supp}A \end{array} \right\}.$$

Recall that given a place P of a function field $F/\mathbb{F}$, $\alpha \in G(P)$ if and only if $\ell(\alpha P) = \ell(\alpha P)$ if and only if there exists $f \in F$ such that $(f)_\infty = \alpha P$. We are interested in the analogous relationships (or lack thereof) in the case of a finite graph. Thus, we let

$$G_f(P) = \mathbb{N} \setminus H_f(P)$$

and

$$G_r(P) = \mathbb{N} \setminus H_r(P).$$

Now, applying Theorem 31, we can obtain a result similar to the classical Weierstrass gap theorem.

Proposition 32. *If $\alpha \geq 2g$, $\alpha \in H_r(P)$. Hence, $G_r(P)$ is finite. In fact,*

$$|G_r(P)| = g.$$

We obtain the following result detailing the relationship between $H_r(P)$ and $H_f(P)$.

Proposition 33. *Let G be a graph and P be a vertex of G. Then,*

$$H_r(P) \subseteq H_f(P).$$

Proof. Let $\alpha \in H_r(P)$. Then, $r((\alpha-1)P) = k$ and $r(\alpha P) = k+1$. Thus, since $r((\alpha-1)P) = k$, there exists $E_0 \in Div_+^{k+1}(G)$ so that for all $f \in \mathcal{M}(G)$, $(\alpha-1)P - E_0 + \Delta(f) \ngeq 0$.

Now, for all $E \in Div_+^{k+1}(G)$, there exists $f \in \mathcal{M}(G)$ so that $\alpha P - E + \Delta(f) \geq 0$. Thus, there exists $h \in \mathcal{M}(G)$ so that $\alpha P - E_0 + \Delta(h) \geq 0$. Thus, it must be that $\Delta_P(h) = \alpha$ and $\Delta_v(h) \geq 0$ for all $v \in V(G) \setminus \{P\}$. Hence, $\alpha \in H_f(P)$. $\square$

Corollary 34. *Let G be a graph and P be a vertex of G. Then, $G_f(P) \subseteq G_r(P)$. Hence, $G_f(P)$ is finite and $|G_f(P)| \leq g$.*

Since $H(P)$ is a semigroup in the function field case, it is natural to as if $H_r(P)$ and $H_f(P)$ are semigroups. We can prove the following.

Proposition 35. *If $\alpha, \beta \in H_f(P)$, $\alpha + \beta \in H_f(P)$.*

Proof. Since $\alpha, \beta \in H_f(P)$, there exist f_1, f_2 such that $\Delta(f_1) = A_1 - \alpha P$ and $\Delta(f_2) = A_2 - \beta P$ where $A_1, A_2 \geq 0$. Now, note that $\Delta_v(f) = \sum_{w \in Nbhd(v)} (f(v) - f(w))$. Thus,

$$\Delta_v(f_1 + f_2) = \sum_{w \in Nbhd(v)} ((f_1 + f_2)(v) - (f_1 + f_2)(w)).$$

Hence,

$$\Delta_v(f_1 + f_2) = \sum_{w \in Nbhd(v)} (f_1(v) - f_1(w)) + \sum_{w \in Nbhd(v)} (f_2(v) - f_2(w)).$$

Thus, we may conclude that

$$\Delta(f_1 + f_2) = \Delta(f_1) + \Delta(f_2),$$

that is, $\alpha + \beta \in H_f(P)$. $\square$

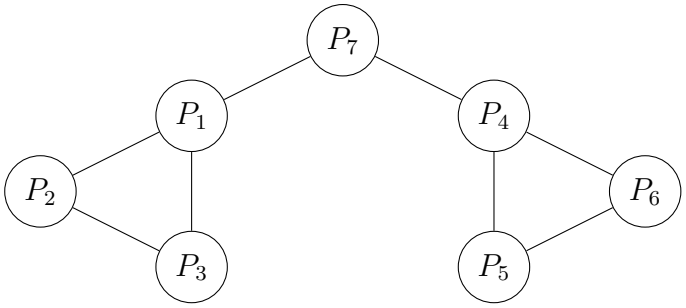
It remains to determine the algebraic structure of $H_f(P)$, if there is any.

While in the function field case, we have the equivalence $\alpha \in H(P)$ if and only if $\ell(\alpha P) = \ell(\alpha P)$ if and only if there exists $f \in F$ such that $(f)_\infty = \alpha P$, it is not the case that $H_r(P) = H_f(P)$. The following examples illustrate this.

Example 15. Consider the graph G in Example 14. Note that $g = 1$, i.e., we know that $1 \in G_r(P)$ for all $P \in V(G)$. Now, consider the function f defined by $f(P_1) = -1$ and $f(P_i) = 0$ for $i = 2, 3, 4$. Then, $\Delta(f) = P_2 - P_1$. Hence, $1 \in H_f(P)$, i.e., $H_r(P) \neq H_f(P)$.

While it may seem that $1 \in H_f(P)$ can only occur if G has a leaf, a second example shows that such problems may arise even if G does not contain a leaf.

Example 16. Consider the graph G shown below.



Note that $g = 2$. Then, $1 \in G_r(P)$ for all $P \in V(G)$.

Now, consider $f \in \mathcal{M}(G)$ where $f(P_i) = 0$ for $i = 1, 2, 3, 7$ and $f(P_i) = 1$ for $i = 4, 5, 6$. Then, $\Delta(f) = P_5 - P_7$. Thus, $1 \in H_f(P_7)$.

These examples show several cases in which $H_f(P) \neq H_r(P)$ for some $P \in V(G)$. We now turn our attention to several cases in which we obtain equality. We consider several families of regular graphs. Specifically, we consider the complete graph on n vertices K_n, the cycle on n vertices C_n and complete bipartite graphs $K_{m,n}$.

In order to show equality, we will make extensive use of a certain set of functions in $\mathcal{M}(G)$. Specifically, we will be interested in a set of indicator functions.

Definition 27. Let G be a graph with vertex set $V(G) = \{P_1, P_2, \ldots, P_n\}$. The indicator function f_{P_i} is defined by

$$f_{P_i}(P_j) = \begin{cases} -1 & \text{if } i = j \\ 0 & \text{otherwise} \end{cases}.$$

Then, consider the set

$$B = \{f_{P_1}, f_{P_2}, \ldots, f_{P_n}\}.$$

Note that

$$\Delta(f_{P_i}) = \sum_{j=1}^{\deg(P_i)} Q_j - \deg(P_i)P_i,$$

where the vertices Q_j are the distinct neighbors of P_i.

Note that these indicator functions represent a single vertex firing in a chip-firing game. When we consider $\Delta_P(f)$, we see that each neighbor of P is gaining a single "zero" and P has a "pole" of order $\deg(P)$. Furthermore, we have the following useful result.

Lemma 36. *Consider a graph G. Then, if $h \in \mathcal{M}(G)$, $h = \sum_B \alpha_{P_i} f_{P_i}$, where $\alpha_i \in \mathbb{Z}$ for all i.*

Proof. Let $h \in \mathcal{M}(G)$ and let $\alpha_w = -h(w)$ for $w \in V(G)$. Then,

$$\begin{aligned} (\textstyle\sum_B \alpha_{P_i} f_{P_i})(w) &= \textstyle\sum_B \alpha_{P_i} f_{P_i}(w) \\ &= \textstyle\sum_{B \setminus \{f_w\}} \alpha_{P_i} f_{P_i}(w) + \alpha_w f_w(w) \\ &= 0 + \alpha_w f_w(w) \\ &= \alpha_w(-1) \\ &= h(w) \end{aligned}$$

Since this argument holds for all w, $h = \sum_B \alpha_{P_i} f_{P_i}$. □

Proposition 37. *Let G be a graph and P be a vertex of G such that $G' = G \setminus \{P\}$ is connected. Then,* $\deg(P)$ *is the smallest nonzero element of $H_f(P)$.*

Proof. Note by the proof of Lemma 39, we know that for a graph G, $\deg(P) \in H_f(P)$. It remains to show it is the minimum nonzero element of $H_f(P)$.

Suppose $c \in H_f(P) \setminus \{0\}$ and $c < \deg(P) = d$. Hence, we may assume $h \in M(G)$. such that $\Delta(h) = A - cP$, where $A \geq 0$. We may assume $h(w) \leq 0$ for all $w \in V(G)$ by the following argument. Note that if $k \in \mathbb{Z}$, $\Delta(h) = \Delta(h + k)$; thus, we consider $v \in V(G)$ so that

$$h(v) = \max\{h(w) | w \in V(G)\}.$$

Then, if $(h - h(v))(P_i) \leq 0$ for $P_i \in V(G)$ and $\Delta(h) = \Delta(h - h(v))$. Thus, $\Delta_P(h) = \sum_w \alpha_w - \alpha_P \deg(P)$, where w is a neighbor of P.

Let $v \in V(G)$ be chosen so that $\alpha_v = \max\{\alpha_w | w \in V(G) \setminus \{P\}\}$. Note that we may assume $\alpha_v > \alpha_w$ where v and w are neighbors. To see this is the case note that since G' is connected $\alpha_w \not> \alpha_v$ for some $w \in V(G) \setminus \{P\}$ implies $\alpha_w = \alpha$ for all $w \in V(G) \setminus \{P\}$. Thus, $\Delta_P(h) = \sum_w \alpha_w - \alpha_P \deg(P) = \deg(P)(\alpha - \alpha_w)$. Thus, $\deg(P) | \Delta_P(h)$ which is a contradiction.

Case 1: v is not a neighbor of P.

Then, $\Delta_P(h) = \sum_{Q_i} \alpha_{Q_i} - \alpha_v \deg(v)$, where $\{Q_i\}$ is the set of neighbors of v.

Hence,

$$\begin{aligned} \Delta_v(h) &= \sum_{Q_i} \alpha_{Q_i} - \alpha_v \deg(v) \\ &= \sum_{Q_i} (\alpha_{Q_i} - \alpha_v) \\ &< 0. \end{aligned}$$

Since $\alpha_v \geq \alpha_{Q_i}$ for all i and $\alpha_v > \alpha_{Q_i}$ for at least one i.

Case 2: v is a neighbor of P.

By assumption, $\sum_w \alpha_w - \alpha_P \deg(P) = -c$. Thus, $\sum_w \alpha_w = \alpha_P \deg(P) - c$. Now, suppose that $\alpha_v < \alpha_P$. Then, $\sum_w \alpha_w < \sum_w \alpha_v \leq (\alpha_P - 1)\deg(P)$ which is a contradiction. Hence, it must be that $\alpha_v \geq \alpha_P$. Thus, if the set of neighbors of v is $\{P, Q_1, Q_2, \ldots, Q_{\deg(v)-1}\}$, we have the following:

$$\begin{aligned}\Delta_v(h) &= \sum_{Q_i} \alpha_{Q_i} + \alpha_P - \alpha_v \deg(v) \\ &= \sum_{Q_i} (\alpha_{Q_i} - \alpha_v) + \alpha_P - \alpha_v \\ &< 0.\end{aligned}$$

Hence, $c \notin H_f(P)$. $\square$

Note that this result also demonstrates that if $c \in H_r(P)$, $c \geq \deg(P)$. Furthermore, applying the previous proposition to C_n gives us the following result.

Proposition 38. *Consider the cycle C_n. Then,*

$$H_r(P) = H_f(P) = \langle 2, 3 \rangle$$

for all $P \in V(C_n)$.

Proof. Consider $P \in V(C_n)$. By the Riemann-Roch theorem for finite graphs and the fact that $g = 1$, we know that if $\alpha \geq 2$, $\alpha \in H_r(P)$. Thus, $H_r(P) = \langle 2, 3 \rangle$.

Now, since $H_r(P) \subseteq H_f(P)$, $\langle 2, 3 \rangle \subseteq H_f(P)$. It remains to show that $1 \notin H_f(P)$.

We know that $\deg(P) = 2$ is the minimum element of $H_f(P) \setminus \{0\}$ since $C_n \setminus \{P\}$ is connected. Thus, $1 \notin H_f(P)$. $\square$

Since C_n is regular, this motivates us to consider several other regular graphs. The next candidate is K_n. First, we show the following lemma which will be of some use later.

Lemma 39. *Consider the complete graph, K_n. Then, $\langle n-1, n \rangle \subseteq H_f(P)$ for all $P \in V(K_n)$.*

Proof. Note that by Proposition 37, $n - 1 \in H_f(P)$.

Now, consider $f = f_{P_1} - f_{P_2}$ where $P_1, P_2 \in V(G)$. Then,

$$\Delta_{P_1}(f) = -1 \deg(P_1) - 1$$

and

$$\Delta_w(f) \geq 0$$

for all $w \in V(G) \setminus \{P_1\}$. Thus, $n \in H_f(P)$. The desired result then follows by Proposition 35. $\square$

If $\alpha \notin \langle n-1, n\rangle$, then $\alpha = i(n-1) + j$ where $0 \leq i < j \leq n-2$. Now, note that if $\alpha \notin \langle n-1, n\rangle$, then α must be element of the following triangle.

$$\begin{array}{ccccccc}
1 & 2 & 3 & \cdots & n-4 & n-3 & n-2 \\
n+1 & n+2 & n+3 & \cdots & 2n-4 & 2n-3 & \\
2n+1 & 2n+2 & 2n+3 & \cdots & 3n-4 & & \\
\vdots & & & \iddots & & & \\
\vdots & & \iddots & & & & \\
\vdots & \iddots & & & & & \\
(n-1)n+1 & & & & & &
\end{array}$$

Thus, $\alpha = kn + l$ where $1 \leq l \leq n-2-k$ and $0 \leq k \leq (n-1)$. Rewriting this we get that $k(n-1) + l + k$. Hence, if $i = k$ and $j = l + k$, we get that $0 \leq i < j \leq n-2$. We may conclude that if $\alpha \notin \langle n-1, n\rangle$, then $\alpha = i(n-1) + j$ where $0 \leq i < j \leq n-2$. Counting these elements we get there are $\frac{(n-1)(n-2)}{2}$ gaps of $\langle n-1, n\rangle$. We now have enough information to show the desired result for K_n.

Proposition 40. *If $G = K_n$ and $P \in V(G)$,*

$$H_r(P) = H_f(P) = \langle n-1, n\rangle.$$

Proof. We show that $H_f(P) = \langle n-1, n\rangle$ and the proposition follows. Note that by Lemma 39, $\langle n-1, n\rangle \subseteq H_f(P)$.

First, note that $g = |E(G)| - |V(G)| + 1$. Since $|V(G)| = n$ and $|E(G)| = \frac{n(n-1)}{2}$, $g = \frac{n(n-1)}{2} - n + 1$. Thus, we have the following.

$$\begin{aligned} g &= \tfrac{n(n-1)}{2} - n + 1 \\ &= \tfrac{n(n-1)}{2} - (n-1) \\ &= \tfrac{n(n-1)-2(n-1)}{2} \\ &= \tfrac{(n-1)(n-2)}{2}. \end{aligned}$$

Hence, if $H_f(P) = \langle n-1, n\rangle$, $H_f(P) = H_r(P)$.

Suppose $\alpha \in H_f(P)$ and $\alpha \notin \langle n-1, n\rangle$, i.e., there exists an $h \in \mathcal{M}(G)$ such that $\Delta(h) = A - \alpha P$ where $A \geq 0$. Then, $\alpha = i\deg(P) + j$ where $0 \leq i < j \leq n-2$ by the previous argument. Note, as above, we may assume that $h(v) \leq 0$ for all $w \in V(G)$, i.e., $\alpha_w \geq 0$ for all $v \in V(G)$.

Now, using the construction of h given in Lemma 36, we get that

$$\Delta(h) = \sum_v \left(\sum_{w \neq v} \alpha_w - \alpha_v \deg(v) \right) v.$$

By assumption, we have

$$\sum_{w \neq P} \alpha_w - \alpha_P \deg(P) = -i\deg(P) - j$$

where $0 \leq i < j \leq \deg(P) - 1$, i.e., $\sum\limits_{w \neq P} \alpha_w \equiv -j \mod \deg(P)$.

Since $h(w) \leq 0$ for $w \in V(G)$, $\alpha_v \geq 0$ for all $v \in V(G)$, i.e., $\sum\limits_{w \neq P} \alpha_w \neq -j$. Thus, it must be that $\sum\limits_{w \neq P} \alpha_w = l(n-1) - j$ where $l > 0$.

Now, since $l \geq 1$ and $\sum_{w \neq P} \alpha_w - \alpha_P \deg(P) = -i\deg(P) - j$, $\alpha_p = i + l$. Choose v so that $\alpha_v = \max\{\alpha_w | w \in V(G) \setminus \{P\}\}$. Recall that $\alpha_v > 0$ by assumption.

Consider $\Delta_v(h)$. Then,

$$\begin{aligned}
\Delta_v(h) &= \sum_{w \neq v,P} \alpha_w + \alpha_P - \alpha_v(n-1) \\
&= \sum_{w \neq P} \alpha_w - \alpha_v + \alpha_P - \alpha_v(n-1) \\
&= -j + l(n-1) + i + l - \alpha_v(n) \\
&= i - j + l(n) - \alpha_v(n) \\
&= i - j + (l - a_v)(n)
\end{aligned}$$

Suppose $\alpha_v \leq l - 1$. Thus,

$$\sum_{w \neq P} \alpha_w \leq \sum_{i=1}^{deg(P)} a_v \leq \sum_{i=1}^{deg(P)} (l-1) = (l-1)\deg(P) < -j + l\deg(P),$$

which is a contradiction.

Hence, $\alpha_v \geq l$. Since $i - j < 0$ and $l - a_v \leq 0$, $\Delta_v(h) < 0$ which contradicts that $\Delta(h) = A - \alpha P$ where $A \geq 0$. Thus, it must be that no such α exists. Therefore, $H_f(P) = \langle n-1, n \rangle$. $\square$

Lemma 41. *Consider the complete bipartite graph $K_{m,n}$ and let (U, V) be the natural partition of the vertices of $K_{m,n}$ where $|U| = m$ and $|V| = n$. Then, if $P \in U$,*

$$\langle n, (m-1)n + 1, (m-1)n + 2, \ldots, (m-1)n + (n-1) \rangle \subseteq H_f(P).$$

Similarly if $P \in V$,

$$\langle m, (n-1)m + 1, (n-1)m + 2, \ldots, (n-1)m + (m-1) \rangle \subseteq H_f(P).$$

Proof. We show this for $P \in U$ as the argument is similar for $P \in V$. Let $V = \{Q_1, \ldots, Q_n\}$

and $U = \{P, P_1, \ldots, P_{m-1}\}$.

Consider the set of indicator functions B defined on G, i.e., $f_v(v) = -1$ and $f_v(w) = 0$ for all $w \in V(G) \setminus \{v\}$. Then,

$$\Delta_{Q_i}(f_P) = 1$$

for $Q \in V$,

$$\Delta_{P_i}(f_P) = 0$$

for $P_i \in U \setminus \{P\}$, and

$$\Delta_P(f_P) = -n.$$

Thus, $n \in H_f(P)$.

Next, we consider $h = mf_P + \sum_{i=1}^{l} f_{Q_i}$, where $1 \leq l \leq n-1$. Thus, $1 \leq n-l \leq n-1$.

Note the following:

$$\begin{aligned}
\bullet\ \Delta_{Q_j}(h) &= m\Delta_{Q_j}(f_P) + \sum_{i=1}^{l} \Delta_{Q_j}(f_{Q_i}) \\
&= 0, \text{ where } 1 \leq j \leq l \\
\bullet\ \Delta_{Q_j}(h) &= m - 0 \text{ where } j > l \\
\bullet\ \Delta_{P_i}(h) &= l, \text{ and} \\
\bullet\ \Delta_P(h) &= m\Delta_{Q_j}(f_P) + \sum_{i=1}^{l} \Delta_{Q_j} f_{Q_i} \\
&= -mn + l \\
&= -((m-1)n + n - l).
\end{aligned}$$

Hence, since $\Delta_v(h) \geq 0$ for $v \in V(G) \setminus \{P\}$, we obtain the desired result by applying Proposition 35. $\square$

Now, consider $a \in \mathbb{Z} \cap [1, (m-1)n]$ and let

$$N = \langle n, (m-1)n+1, (m-1)n+2, \ldots, (m-1)n+(n-1) \rangle.$$

Note that if $a \in N$, $n|a$. Thus, the gaps of N are

$$\{in + j | 0 \leq i \leq m-2,\ 1 \leq j \leq n-1\}.$$

We can apply our results to $K_{m,n}$ to obtain the following result.

Lemma 42. *Consider $K_{m,n}$ and let (U, V) be the natural partition of the vertices of $K_{m,n}$ where $|U| = m$ and $|V| = n$. Then, if $P \in U$,*

$$H_f(P) = H_r(P) = \langle n, (m-1)n+1, (m-1)n+2, \ldots, (m-1)n+(n-1) \rangle.$$

Similarly, if $P \in V$,

$$H_f(P) = H_r(P) = \langle m, (n-1)m+1, (n-1)m+2, \ldots, (n-1)m+(m-1) \rangle.$$

Proof. We show this for $P \in U$ as the argument is similar for $P \in V$. Let $V = \{Q_1, \ldots, Q_n\}$ and $U = \{P, P_1, \ldots, P_{m-1}\}$.

Let $N = \langle n, (m-1)n+1, (m-1)n+2, \ldots, (m-1)n+(n-1) \rangle$. Note that by Lemma 41, $N \subseteq H_f(P)$. Furthermore, note that the genus of $K_{m,n}$ is $g = |E(G)| - |V(G)| + 1$. Thus, $g = mn - (m+n) + 1 = (m-1)(n-1)$. Now, note that

$$|\mathbb{N} \setminus N| = (m-1)n - (m-1) = (m-1)(n-1) = g$$

by Lemma 41.

Thus, if we can show that $N = H_f(P)$, the theorem is proved. Suppose that

$$N \subsetneqq H_f(P),$$

that is, there exists $\alpha \in H_f(P)$ but $\alpha \notin N$. Hence, there exists $h \in M(G)$ so that $\Delta(h) = A - \alpha P$, $P \notin \mathit{supp}\ A$, $A \geq 0$. Note, as above, we may assume that $h(w) \leq 0$ for all $w \in V(G)$, i.e., $\alpha_w \geq 0$ for all $w \in V(G)$.

As before, we have $\Delta(h) = \sum_v \left(\sum_{w \in Nbhd(v)} \alpha_w - \alpha_v \deg(v) \right) v$. Furthermore, we know $\alpha = in + j$ where $0 \leq i \leq m-2,\ 1 \leq j \leq n-1$. Combining these facts,

$$\sum_{i=1}^{n} \alpha_{Q_i} - \alpha_P n = -in - j.$$

Hence,

$$\sum_{i=1}^{n} \alpha_{Q_i} \equiv -j \mod n.$$

Since $\alpha_{Q_i} \geq 0$ for all i, $\sum_{i=1}^{n} \alpha_{Q_i} = ln - j$ where $l \geq 1$. Thus, it must be that $l - \alpha_P = -i$, i.e., $l + i = \alpha_P$. Let $v \in V(G)$ be chosen so that $\alpha_v = \max \{\alpha_w | w \in V(G) \setminus \{P\}\}$.

Now, we consider two cases.

Case 1: Suppose $v = P_i$ for some $P_i \in U$.

Then, we have the following:

$$\begin{aligned} \Delta_{P_i}(h) &= \sum_{i=1}^{n} \alpha_{Q_i} - \alpha_{P_i} n \\ &= lm - j - \alpha_{P_i} n \\ &= -j + (l - \alpha_{P_i}) n. \end{aligned}$$

We claim that $\alpha_{P_i} \geq l$. Suppose instead that $\alpha_{P_i} \leq l - 1$. Then, $\sum_{i=1}^{n} \alpha_{Q_i} \leq \sum_{i=1}^{n} (l-1) = ln - n < ln - j$, which is a contradiction. Thus, the claim holds.

Hence, $\Delta_{P_i}(h) \leq -j$, which contradicts that $\Delta_{P_i}(h) \geq 0$.

Case 2: Suppose $v = Q_j$ for some $Q_j \in V$.

Consider $\Delta_{Q_j}(h) = \sum_{i=1}^{m-1} P_i + \alpha_P - \alpha_{Q_j} m$. We may assume that $\alpha_{Q_j} > \alpha_{P_i}$; otherwise

we may apply Case 1. Hence, $\alpha_{P_i} - \alpha_{Q_j} \leq -1$. Also, note as in Case 1, it must be that $\alpha_{Q_j} \geq l$, and $l + i = \alpha_P$, i.e., $\alpha_P \leq \alpha_{Q_j} + i$.

Then,

$$\begin{aligned}
\Delta_{Q_j}(h) &= \sum_{i=1}^{m-1} P_i + \alpha_P - \alpha_{Q_j} m \\
&= \alpha_P - \alpha_{Q_j} + \sum_{i=1}^{m-1} (P_i - \alpha_{Q_j}) \\
&\leq \alpha_{Q_j} + i - \alpha_{Q_j} - (m-1) \\
&= i - (m-1) \\
&< 0.
\end{aligned}$$

Thus, it must be that such an α does not exist. Therefore, $H_f(P) = H_r(P) = \langle n, (m-1)n+1, (m-1)n+2, \ldots, (m-1)n+(n-1)\rangle$. $\square$

We immediately have the following result.

Theorem 43. *Consider the complete bipartite graph $K_{m,m}$. Then, for any $P \in V(K_{m,m})$,*

$$H_f(P) = H_r(P) = \langle m, (m-1)m+1, (m-1)m+2, \ldots, m^2-1\rangle.$$

In [2], the authors introduced the idea of a Weierstrass semigroup of multiple points. We extend these definitions to multiple vertices on a finite graph in the next definition.

Definition 28. Let G be a graph and $P \in V(G)$. Then,

$$H_r(P_1, P_2, \ldots, P_m) = \left\{ \alpha \in \mathbb{N} \ : \ \begin{array}{l} r\left(\sum_{i=1}^m \alpha_i P_i\right) = r\left(\left(\alpha_j - 1\right) P_j + \sum_{i=1, i\neq j}^m \alpha_i P_i\right) + 1, \\ \text{for all } 1 \leq j \leq m \end{array} \right\}$$

and

$$H_f(P_1, P_2, \ldots, P_m) = \left\{ \alpha \in \mathbb{N}^m : \ \begin{array}{l} \text{there exists } f \in \mathcal{M}(G) \text{ such that} \\ \Delta(f) = A - \sum_{i=1}^n \alpha_i P_i \text{ where } A \geq 0 \text{ and } P \notin \text{supp} A \end{array} \right\}.$$

Since we know that $H_r(P) \subseteq H_f(P)$, one might conjecture that

$$H_r(P_1, P_2, \ldots, P_m) \subseteq H_f(P_1, P_2, \ldots, P_m).$$

However, the following example shows this fails in general.

Example 17. Let $G = K_5$. Then, using the Laplacian we can compute $H_f(P_1, P_2)$. Specifically, by finding the Smith Normal Form of the Laplacian, we can solve the equation $Q[f] = [\Delta(f)]$, where $\Delta_{P_1}(f), \Delta_{P_2}(f) \leq 0$ and $\Delta_{P_i}(f) \geq 0$ for $i \neq 1, 2$. The graph in Figure 5.1 shows ordered pairs (α, β) such that $(\alpha, \beta) \in H_f(P_1, P_2)$. The line occurs at $\alpha+\beta = 2g-1$. Note that if $\alpha+\beta > 2g$, $(\alpha, \beta) \in H_r(P_1, P_2)$. Hence, $H_f(P_1, P_2) \not\subseteq H_f(P_1, P_2)$.

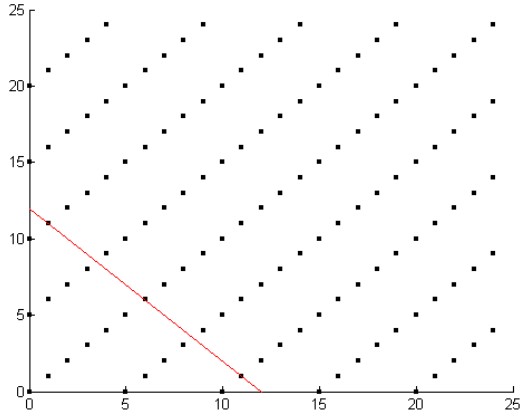


Figure 5.1: $H_f(P_1, P_2)$ for $P_1, P_2 \in V(K_5)$

5.3 Conclusion

In this chapter, we have considered two possible generalizations of Weierstrass semigroups to finite graphs. We have seen that in the case of a single vertex $H_r(P) \subseteq H_f(P)$. In certain special cases, we have found equality and specific generators for the resulting

semigroup. This definition extends to more than one vertex, but we may conclude even less about structure of the two sets.

Chapter 6

Suzuki-invariant codes from the Suzuki curve

This chapter contains joint work which was conducted at the Mathematics Department, Colorado State University in Summer 2011, funded by NSF grant DMS-11-01712. This work is the result of collaboration with Abdulla Eid, Hilaf Hasson, and Amy Ksir.

The Suzuki curve has been a source of very good error-correcting codes. Codes constructed from the Suzuki curve have been studied in [17] , [7] (one-point codes) and [26] (two point codes) and shown to have very good parameters. Furthermore, this curve has a very large automorphism group for its genus, namely the Suzuki group $\mathrm{Sz}(q)$.

6.1 Preliminaries

Let $m \geq 1$ be an integer, $q_0 = 2^m$, $q = 2^{2m+1} = 2q_0^2$, and X_m denote the projective curve defined by the affine equation

$$f_m := z^q + z - y^{q_0}(y^q + y)$$

over the field $\mathbb{F}_q$ of q elements. Then, X_m has a plane projective model in $\mathbb{P}^2(\mathbb{F}_q)$ with the homogeneous equation

$$z^q u^{q_0} + z u^{q+q_0-1} = y^{q+q_0} + y^{q_0+1} u^{q-1}$$

and homogeneous coordinates $[u : y : z]$. This curve has been studied, for example, in [8] and [18] and it has been shown in [14] that the curve has a smooth embedding in projective space. It has a very large automorphism group for its genus, namely the Suzuki group $\mathrm{Sz}(q)$ of order $q^2(q-1)(q^2+1)$. For this reason, it is known as the Suzuki curve. The following facts were established in [17]:

Proposition 44. *1. X_m has only one point at infinity $P_\infty \in X_m \cap \{u = 0\}$ namely $P_\infty = [0 : 0 : 1]$.*

2. The number of rational $\mathbb{F}_q$-points of X_m is $q^2 + 1$. Thus, X_m is maximal.

3. The functions y, z, $h_1 := y^{2q_0+1} + z^{2q_0}$ and $h_2 := yz^{2q_0} + h_1^{2q_0}$ are regular except at P_∞, where their pole orders are q, $q + q_0$, $q + 2q_0$, and $q + 2q_0 + 1$ respectively.

4. The genus of X_m is $q_0(q-1)$.

Let F_m be the function field defined by the affine equation f_m of the curve X_m over $\mathbb{F}_{q^4}(y)$. Let $P'_\infty \in \mathbb{P}_{\mathbb{F}_q(y)}$ be the place at infinity of $\mathbb{F}_q(y)$. The place P_∞ of F_m that lies above P'_∞ is a ramified place with ramification index $e(P_\infty \mid P'_\infty) = q$. All affine places P_α of $\mathbb{F}_q(y)$ are unramified, and each splits completely in F_m to $P_{\alpha,\beta}$ ($\beta \in \mathbb{F}_q$). We will denote the valuations corresponding to P_∞ and $P_{\alpha,\beta}$ by ν_∞ and $\nu_{\alpha,\beta}$ respectively.

Let $\mathcal{P} \subseteq \mathbb{N}$ be the monoid generated by the pole orders of the functions y, z, h_1, h_2 defined above, meaning

$$\mathcal{P} := \langle q, q+q_0, q+2q_0, q+2q_0+1 \rangle \subseteq \mathbb{N}.$$

We notice that if $n \in \mathcal{P}$, then $n = aq + b(q + q_0) + c(q + 2q_0) + d(q + 2q_0 + 1)$ for some $a, b, c, d \in \mathbb{N}$. Set $f_n := y^a z^b h_1^c h_2^d$. Then in [17], the authors show

$$\mathcal{L}(dP_\infty) = Span\ \{f_n \mid n \in \mathcal{P}, n \leq d\}.$$

The action of the Suzuki group $\mathrm{Sz}(q)$ is generated by

$$Sz(q) = \left\langle \begin{pmatrix} 1 & 0 & 0 \\ \alpha & 1 & 0 \\ \gamma & \alpha^{2q_0} & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 & 1 \\ 0 & \xi & 0 \\ 0 & 0 & \xi^{q_0+1} \end{pmatrix}, \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix} \mid \alpha, \gamma \in \mathbb{F}_q, \xi \in \mathbb{F}_q^\times \right\rangle$$

where the first matrix corresponds to the Sylow 2-subgroup of order q^2 generated by the automorphism that sends $y \mapsto y + \alpha$ and $z \mapsto z + \alpha^{q_0} y + \gamma$, where $\alpha, \gamma \in \mathbb{F}_q$ and the second matrix correspond to subgroup of order $q - 1$ generated by $y \mapsto \xi y$ and $z \mapsto \xi^{q_0+1} z$, where $\xi \in \mathbb{F}_q^*$ and the third matrix is the automorphism that moves the point at infinity. Note that for the affine points on the Suzuki curve, the automorphisms $\sigma : y \mapsto y + a$ and $\sigma : z \mapsto z + a^{q_0} y + \gamma$ will act on the affine $\mathbb{F}_q$-points transitively and freely.

Remark 3. If $(y, z) \in X_m$, then $z^q + z = y^{q_0}(y^q + y)$ and

$$\begin{aligned} \sigma(z^q + z) &= \sigma(z)^q + \sigma(z) \\ &= (z + a^{q_0} y + \gamma)^q + (z + a^{q_0} y + \gamma) \\ &= z^q + a^{q_0 q} y^q + \gamma^q + z + a^{q_0} y + \gamma \\ &= (z^q + z) + a^{q_0 q} y^q + a^{q_0} y + (\gamma^q + \gamma) \\ &= (z^q + z) + a^{q_0}(y^q + y). \end{aligned}$$

Conversely,

$$\begin{aligned} \sigma(y^{q+q_0} + y^{q_0+1}) &= \sigma(y)^{q_0+q} + \sigma(y)^{q_0+1} \\ &= (y + a)^{q_0+q} + (y + a)^{q_0+1} \\ &= y^{q_0+q} + y^{q_0+1}. \end{aligned}$$

The number $N_i(X_m)$ of $\mathbb{F}_{q^k}$-rational points on the curve can be determined using its zeta function. If $L(X_m, t) = \prod_{j=1}^{2g}(1 - w_j t)$, then

$$N_i(X_m) = q^i + 1 - \sum_{j=1}^{2g} w_j^i. \tag{6.1}$$

For the Suzuki curve above,

$$L(t) = (q + 2q_0 t + t^2)^g,$$

and the reciprocals of the roots of $L(t)$ are $\underbrace{\alpha, \alpha, \cdots, \alpha}_{g \text{ times}}$ and $\underbrace{\beta, \beta, \cdots, \beta}_{g \text{ times}}$, where

$$\alpha := 2^m(-1 + i)$$

and

$$\beta := \bar{\alpha} = 2^m(-1 - i).$$

6.2 The Riemann-Roch space $\mathcal{L}(\ell D)$

Consider the divisor $D \in \mathrm{Div}(X_m)$ given by the sum of all rational $\mathbb{F}_q$-points of X_m, i.e., $D = \sum_{\alpha,\beta \in \mathbb{F}_q} P_{\alpha,\beta} + P_\infty$. Since there are $q^2 + 1$ rational points of X_m, $\deg(D) = q^2 + 1$. We also note that this divisor has the property that D is fixed by $\mathrm{Sz}(q)$. Next we find a $\mathbb{F}_q$-basis for the space $\mathcal{L}(\ell D)$ with $\ell \leq q^2 - 1$.

Lemma 45. *Let $\ell \in \mathbb{N}$ and D be defined to be the sum of all rational points of X_m. Then,*

$$S := \left\{ \frac{y^a z^b h_1^c h_2^d}{(y^q + y)^r} : \begin{array}{l} aq + b(q + q_0) + c(q + 2q_0) + d(q + 2q_0 + 1) \leq rq^2 + \ell, \\ 0 \leq a \leq q - 1, 0 \leq b \leq 1, 0 \leq c \leq q_0 - 1, \\ 0 \leq d \leq q_0 - 1, 0 \leq r \leq \ell \end{array} \right\} \subseteq \mathcal{L}(\ell D),$$

and S is a linearly independent set.

Proof. First we show $S \subseteq L(\ell D)$. To see this is the case, note that

$$((y^q + y)^\ell) = ((y^q + y)^\ell)_0 - ((y^q + y)^\ell)_\infty = \ell \sum_{\alpha,\beta \in \mathbb{F}_q} P_{\alpha,\beta} - \ell q^2 P_\infty.$$

Thus, $\ell D = \ell(q^2+1)P_\infty + ((y^q + y)^\ell)$, i.e., $\ell D \simeq \ell(q^2+1)P_\infty$. Thus, we have the $\mathbb{F}_q$-isomorphism

$$\mathcal{L}(\ell D) \simeq \mathcal{L}(\ell(q^2+1)P_\infty).$$

Now let $\frac{y^a z^b h_1^c h_2^d}{(y^q+y)^r} \in S$. We need to show that

$$\frac{y^a z^b h_1^c h_2^d}{(y^q + y)^r} \cdot (y^q + y)^\ell \in \mathcal{L}(\ell(q^2+1)P_\infty).$$

Note that

$$\begin{aligned} -\nu_\infty(y^a z^b h_1^c h_2^d) + (-\ell + r)q^2 + \ell(q^2+1) &= -\nu_\infty(y^a z^b h_1^c h_2^d) - \ell q^2 + r q^2 + \ell q^2 + 1 \\ &= \ell + r q^2 \\ &\geq 0. \end{aligned}$$

Hence, $\frac{y^a z^b h_1^c h_2^d}{(y^q+y)^{\ell-r}} \in \mathcal{L}(\ell(q^2+1)P_\infty)$, i.e., $\frac{y^a z^b h_1^c h_2^d}{(y^q+y)^r} \in \mathcal{L}(\ell D)$. Thus, $S \subseteq \mathcal{L}(\ell D)$.

Next, to show the functions of S are independent we show that the valuations at the point at infinity are unique.

Let $f_1, f_2 \in S$ where $f_1 = \frac{y^{a_1} z^{b_1} h_1^{c_1} h_2^{d_1}}{(y^q+y)^{r_1}}$ and $f_2 = \frac{y^{a_2} z^{b_2} h_1^{c_2} h_2^{d_2}}{(y^q+y)^{r_2}}$. Suppose $v_\infty(f_1) = v_\infty(f_2)$. Then,

$$\begin{aligned} &-[a_1 q + b_1(q+q_0) + c_1(q+2q_0) + d_1(q+2q_0+1)] + r_1 q^2 = \\ &-[a_2 q + b_2(q+q_0) + c_2(q+2q_0) + d_2(q+2q_0+1)] + r_2 q^2 \end{aligned} \tag{6.2}$$

Now consider (6.2) modulo q_0. Then,

$$d_1 \equiv d_2 \mod q_0.$$

Now, since $1 \leq d_1, d_2 \leq q_0 - 1$, it must be that $d_1 = d_2$.

Next, we consider (6.2) modulo $2q_0$. Then,

$$b_1 q_0 + d_1 \equiv b_2 q_0 + d_1 \mod 2q_0.$$

Note that $0 \leq b_1, b_2 \leq 1$, i.e., $b_1 = b_2$.

Next, consider (6.2) modulo q. Then,

$$b_1 q_0 + 2c_1 q_0 + 2d_1 q_0 + d_1 \equiv b_1 q_0 + 2c_2 q_0 + 2d_1 q_0 + d_1 \mod q.$$

After reducing, we have that $2c_1 q_0 \equiv 2c_2 q_0 \mod q$, i.e., for some $h \in \mathbb{Z}$, $hq = 2c_1 q_0 - 2c_2 q_0$. Note that since $0 \leq c_1, c_2 \leq q_0 - 1$,

$$-q < 2c_1 q_0 - 2c_2 q_0 < q.$$

Thus, it must be that $h = 0$ and $c_1 = c_2$.

Finally, consider (6.2) modulo q^2. Then, since $b_1 = b_2$, $c_1 = c_2$, $d_1 = d_2$, we have

$$a_1 q \equiv a_2 q \mod q^2.$$

Note that $0 \leq a_1, a_2 \leq q - 1$. Thus, it must be that $a_1 = a_2$. This also shows that $r_1 = r_2$. We conclude that $v_\infty(f_1) = v_\infty(f_2)$ implies that $f_1 = f_2$. $\square$

To show that S is a basis for $\mathcal{L}(\ell D)$, all that remains is to show that S spans $L(\ell D)$.

To do that we rely on a result from [17].

Proposition 46. *[[17], Proposition 1.6] Let* $\mathcal{P} = \langle q, q+q_0, q+2q_0, q+2q_0+1\rangle$. *Note that for each* $n \in \mathcal{P}$, *there are functions* f_n *so that* f_n *is regular on* X_m *except at* P_∞, *i.e.,* $v_{P_\infty}(f_n) = -n$. *Choose one such* f_n *for each* $n \in \mathcal{P}$. *Then, for any* $d \in \mathbb{Z}$, $\mathcal{L}(dP_\infty)$ *has as basis the set*

$$\{f_n : n \in \mathcal{P}, n \leq d\}.$$

Lemma 47. *Let* $\ell \in \mathbb{N}$, $\ell \leq q^2 - 1$. *Let* S *be as in Lemma 45. Let* $T = \left\{f(y^q + y)^l : f \in S\right\}$ *and* $V = \{-v_{P_\infty}(f) : f \in T\}$. *Then,* $V = \mathcal{P} \cap \{n \in \mathbb{Z} : n \leq \ell(q^2+1)\}$.

Proof. Let $n \in \mathcal{P} \cap \{n \in \mathbb{Z} \,|\, n \leq \ell(q^2+1)\}$, then we have

$$n = aq + b(q+q_0) + c(q+2q_0) + d(q+2q_0+1) \text{ with } n \leq \ell(q^2+1)$$

Now, we want to find a', b', c', d', r' such that

$$n = a'q + b'(q+q_0) + c'(q+2q_0) + d'(q+2q_0+1) + r'q^2$$

where $0 \leq a' < q, 0 \leq b' < 2, 0 \leq c', d' < q_0, 0 \leq r \leq \ell$. Applying the Euclidean Algorithm to a, b, c, d,

$$a = qt_1 + a', \quad 0 \leq a' < q$$
$$b = 2t_2 + b', \quad 0 \leq b' < 2$$
$$c = q_0 t_3 + c', \quad 0 \leq c' < q_0$$

and

$$d = q_0 t_4 + d', \quad 0 \leq d' < q_0.$$

Now set

$$r' := \ell - \frac{q^2 t_1 + 2(q+q_0)t_2 + q_0(q+2q_0)t_3 + q_0(q+2q_0+1)t_4}{q^2}$$

which satisfies the condition $0 \leq r' \leq \ell$. It remains to show that

$$qa' + b'(q+q_0) + c'(q+2q_0) + d'(q+2q_0+2) \leq r'q^2 + \ell.$$

Note that $n \leq \ell q^2 + \ell$. Thus,

$$\begin{aligned} n = qa' + b'(q+q_0) + c'(q+2q_0) + d'(q+2q_0+2) + (\ell - r')q^2 &\leq \ell q^2 + \ell \\ qa' + b'(q+q_0) + c'(q+2q_0) + d'(q+2q_0+2) &\leq \ell q^2 + \ell + r'q^2 - \ell q^2 \\ &\leq \ell + r'q^2. \end{aligned}$$

Therefore $V = \mathcal{P} \cap \{n \in \mathbb{Z} \,|\, n \leq \ell(q^2+1)\}$. $\square$

Using the two previous lemmas we can now obtain the desired result.

Theorem 48. *Let $\ell \in \mathbb{N}$, $\ell \leq q^2 - 1$, and D be defined to be the sum of all rational points of X_m. Then,*

$$S := \left\{ \frac{y^a z^b h_1^c h_2^d}{(y^q + y)^r} : \begin{array}{l} aq + b(q+q_0) + c(q+2q_0) + d(q+2q_0+1) \leq rq^2 + \ell, \\ 0 \leq a \leq q-1, 0 \leq b \leq 1, 0 \leq c \leq q_0 - 1, \\ 0 \leq d \leq q_0 - 1, 0 \leq r \leq \ell \end{array} \right\}$$

is a basis for $\mathcal{L}(\ell D)$.

Proof. First, note that there is an isomorphism between $\mathcal{L}(\ell D)$ and $\mathcal{L}(\ell(q^2+1)P_\infty)$ given by multiplication by $(y^q+y)^\ell$. Hence, $\dim \mathcal{L}(\ell D) = \dim \mathcal{L}(\ell(q^2+1)P_\infty)$.

Next, note that by Theorem 47, $\#\{f \in S\} = \dim \mathcal{L}(\ell(q^2+1)P_\infty) = \dim \mathcal{L}(\ell D)$. By Theorem 45, S is a linearly independent set of functions. Thus, the result follows. □

Note: Using the isomorphism $\mathcal{L}(\ell D) \simeq \mathcal{L}(\ell(q^2+1)P_\infty)$, one can directly apply results in [17] to find a basis for $\mathcal{L}(\ell D)$. We note that this relies on finding functions to generate the pole orders in $\mathcal{P}$. Theorem 48 allows avoids this problem by providing an explicit construction.

6.3 Construction and properties of the code $C(E, \ell D)$

As above, let $D \in \mathrm{Div}(X_m)$ be the sum of all $\mathbb{F}_q$-points in X_m. By the previous section, if $\ell \leq q^2-1$, $\dim_{\mathbb{F}_q} \mathcal{L}(\ell D) = \ell(q^2+1) - q_0(q-1) + 1$.

Now, consider the field extension $\mathbb{F}_{q^4}$ of $\mathbb{F}_q$, let $E \in \mathrm{Div}(X_m)$ be the divisor consisting of the sum of all $\mathbb{F}_{q^4}$-points minus the sum of all $\mathbb{F}_q$-points. Then, we have

$$\deg(E) = N_4(X_m) - N_1(X_m),$$

where $N_4(X_m)$ is given by (6.1), i.e.,

$$N_4(X_m) = q^4 + 1 - g(\alpha^4 + \beta^4) = q^4 + 1 + 2gq^2 = q^4 + 1 + 2q_0q^2(q-1).$$

Hence, $\deg(E) = q^4 + 1 + 2q_0q^2(q-1) - (q^2+1) = q^4 + 2q_0q^2(q-1) - q^2$.

Since $\mathrm{supp}(E) \cap \mathrm{supp}(D) = \phi$ and Theorem 48 provides bases for $\mathcal{L}(\ell D)$, we can construct the algebraic geometric code using the divisors E and D.

Theorem 49. *Consider*

$$C_{m,\ell} := C_{\mathcal{L}}(E, \ell D),$$

over $\mathbb{F}_{q^4}$ *where* $\ell \leq q^2 - 1$. *This code has length* $q^4 + 2q^2 q_0(q-1) - q^2$, *dimension* $\ell(q^2+1) - q_0(q-1) + 1$, *and minimum distance at least* $n - \ell(q^2+1)$.

Remark 4. Consider the field extension $\mathbb{F}_{q^2}|\mathbb{F}_q$, and let E be the sum of all $\mathbb{F}_{q^2}$-points minus the sum of all $\mathbb{F}_q$-points. Then,

$$\begin{aligned} \deg(E) &= q^2 + 1 - g(\alpha^2 + \beta^2) - q^2 - 1 \\ &= q^2 + 1 - g(-iq + iq) - q^2 - 1 = 0 \end{aligned}$$

A similar argument shows that the extension $\mathbb{F}_{q^3}|\mathbb{F}_q$ yields $\deg(E) = 0$. Thus, the first nontrivial extension to consider is $\mathbb{F}_{q^4}|\mathbb{F}_q$.

Now we turn our attention to the family of codes given by $\ell = q^2 - 1$ and denote this family of codes by C_m, that is, $C_m = C_{m,q^2-1}$. By Theorem 49, C_m has length $q^4 + 2q^2 q_0(q-1) - q^2$, dimension $q^4 - q_0(q-1)$, and minimum distance at least $2q^2 q_0(q-1) - q^2 + 1$. Thus, C_m has information rate

$$R_m := \frac{k_m}{n_m} = \frac{q^4 - q_0 q + q_0}{q^4 + 2q^2 q_0(q-1) - q^2} = \frac{16q_0^8 - 2q_0^3 + q_0}{16q_0^8 + 16q_0^7 - 4q_0^5 - 4q_0^4}.$$

Thus, as $m \to \infty$, i.e., $q \to \infty$, $R_m \to 1$.

Example 18. Let $m = 1$; thus, $q = 8$ and $q_0 = 2$. Then, the resulting code C_1 is a $[5824, 4082, \geq 1729]$ code over $\mathbb{F}_{4096}$, with information rate $R_1 = 0.7008$. We note here that the block length of the code is greater than the field size, i.e., this code cannot be achieved with a Reed-Solomon code and has polynomial time construction.

Example 19. Let $m = 2$; then, $q = 32$ and $q_0 = 4$. Thus, the resulting code C_2 is a $[1051679, 1048452, \geq 3104]$ code over $\mathbb{F}_{1048576}$ with information rate $R_2 = 0.996$.

Remark 5. Recall the matrix representation of the Suzuki group $Sz(q)$ is given previously. We can view the action of the Suzuki group on the curve by the map $\varphi : \mathcal{X}_m \to \mathbb{P}^4(\mathbb{F}_q)$ defined by $\varphi([u : y : z]) = [u : y : z : h_1 : h_2]$. Since the Suzuki group acts transitively and freely on the affine points, the Suzuki group fixes both D and E. Thus, by [35, Theorem 8.2], the Suzuki group $Sz(q^4)$ is a subgroup of $Aut(C_{\mathcal{L}}(E, \ell D))$.

Remark 6. We conclude this section by explaining why permutation decoding (PD) introduced by MacWilliams in [23] is not efficient for our construction. Following [21, 22], in order to apply permutation decoding, one needs to enumerate all code automorphisms that are in the PD-set. In [21, Thm 10.2.2], it is shown that the lower bound of the PD-set P satisfies

$$|P| \geq \left\lceil \frac{n}{r} \left\lceil \frac{n-1}{r-1} \cdots \left\lceil \frac{n-t+1}{n-r+1} \right\rceil \right\rceil \right\rceil$$

where $t = \lfloor \frac{d-1}{2} \rfloor$ and $r = n - k$. Since the code C_m has a relatively small $r = 2q^2q_0(q-1) - q^2 + q_0(q-1)$, the size of the PD-set will be large which in general will make the enumeration of its elements inefficient.

Chapter 7

Conclusion

While there exist algorithms to find Riemann-Roch spaces [19], very little is known on how to find an explicit expression for bases of Riemann-Roch spaces. In this dissertation, we provide explicit bases for a large family of Riemann-Roch spaces on function fields defined by linearized polynomials. We apply these bases to a construction of small-bias sets and to describing Weierstrass semigroups. Moreover, we provide explicit bases for a second family of Riemann-Roch spaces on the Suzuki function field. It remains to finish work on the duals of the codes arising from these bases.

Much is still to be done with the function fields defined by linearized polynomials. It remains to find the zeta function of this family of function fields and apply the results to codes. Furthermore, the right choice of linearized polynomials remains open. Finding linearized polynomials whose splitting field is $\mathbb{F}_{q^r}$ would provide larger families of function fields for codes than those considered here. The techniues utilized here likely apply more broadly and this is a topic of future research

We also consider two possible analogues of the Weierstrass semigroup for a finite graph. We show that for some families of regular graphs that these two analogues yield the same set. It remains to find all families of graphs for which this holds and to find

generalizations to Weierstrass semigroups of m-tuples of vertices.

Bibliography

[1] N. Alon, O. Goldreich, J. Hastad, and R. Peralta. Simple constructions of almost k–wise independent random variables. *Random Structures Algorithms*, 3(3), 1992.

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

[3] M. Baker. Specialization of linear systems from curves to graphs. *Algebra & Number Theory*, 2(6):613–653, 2008.

[4] M. Baker and S. Norine. Riemann-Roch and Abel-Jacobi theory on a finite graph. *Advances in Mathematics*, 215:766–788, 2007.

[5] A. Ben-Aroya and A. Ta-Shma. Constructing small-bias sets from algebraic-geometric codes. In *FOCS '09*, pages 191–197, 2009.

[6] M. Bras-Amoros and M. E. O'Sullivan. Duality for some families of correction capability optimized evaluation codes. *Adv. Math. Commun.*, 2(1):15–33, 2008.

[7] C. Chen and I. Duursma. Geometric Reed-Solomon codes of length 64 and 65 over $\mathbb{F}_8$. *IEEE Trans. Inform. Theory*, 49(5):1351–1353, 2003.

[8] P. Deligne and G. Lusztig. Representations of reductive groups over finite fields. *Ann. of Math.*, 103:103–161, 1976.

[9] I. Duursma, R. Kirov, and S. Park. Distance bounds for algebraic geometric codes. preprint.

[10] I. M. Duursma and S. Park. Coset bounds for algebraic geometric codes. *Finite Fields and Their Applications*, 16(1):36–55, 2010.

[11] G. D. Forney. *Concatenated Codes*. PhD thesis, MIT Press, Cambridge, MA, 1966.

[12] O. Geil. On codes from norm-trace curves. *Finite Fields Appl.*, 9(3):351–371, 2004.

[13] O. Geil and R. Matsumoto. Bounding the number of $\mathbb{F}_q$-rational places in algebraic function fields using Weierstrass semigroups. *J. Pure Appl. Algebra*, 213(6):1152–1156, 2009.

[14] M. Giulietti, G. Korchmáros, and F. Torres. Quotient curves of the Suzuki curve. *Acta Arith.*, 122:245–274, 2006.

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

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

[17] J. P. Hansen and H. Stichtenoth. *Appl. Algebra Engrg. Comm. Comput.*, 1(1):67–77, 1990.

[18] H.W. Henn. Funktionenkörper mit großer automorphismengruppe. *J. Reine Angew. Math.*, 302:96–115, 1978.

[19] F. Hess. Computing Riemann–Roch spaces in algebraic function fields and related topics. *J. Symb. Comp.*, 33(4):425–445.

[20] T. Høholdt, J. H. van Lint, and R. Pellikaan. Algebraic geometry codes. In W. C. Huffman V. Pless and R. A. Brualdi, editors, *Handbook of Coding Theory*, pages 871–961. Elsevier, 1998.

[21] W. C. Huffman and V. Pless. *Fundamentals of error-correcting codes*. Cambridge Univ. Press, 2003.

[22] D. Joyner. Conjectural permutation decoding of some AG codes. *ACM SIGSAM Bulletin*, 39:166–172, 2005.

[23] F. J. MacWilliams. Permutation decoding of systematic codes. *Bell System Tech. J.*, 43:485–505, 1964.

[24] 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*, 195:261–280, 2005.

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

[26] G. L. Matthews. Codes from the Suzuki function field. *IEEE Trans. Inform. Theory*, 50(12):3298–3302, 2004.

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

[28] G. L. Matthews. Weierstrass semigroups and codes from a quotient of the Hermitian curve. *Des. Codes Cryptogr.*, 37(3):473–492, 2005.

[29] G. L. Matthews. On Weierstrass semigroups of some triples on norm-trace curves. *Lecture Notes in Comput. Sci.*, 5557:146–156, 2009.

[30] G. L. Matthews and J. D. Peachey. Explicit bases for Riemann-Roch spaces of the extended norm-trace function field with applications to AG codes. preprint.

[31] C. Munuera, G. C. Tizziotti, and F. Torres. Two-point codes on norm-trace curves. In *ICMCTA '08: Proceedings of the 2nd international Castle meeting on Coding Theory and Applications*, pages 128–136, Berlin, Heidelberg, 2008. Springer-Verlag.

[32] J. Naor and M. Naor. Small bias probability spaces: efficient construction and applications. *SIAM J. Comput.*, 22:838–856, 1993.

[33] H. Stichtenoth. Ober die automorphismengruppe eines algebraischen funktionenkorpers von primzahlcharackteristik, teil 2. *Arch. Math.*, 24:615–631, 1973.

[34] H. Stichtenoth. A note on Hermitian codes over GF (q^2). *IEEE Trans. Inform. Theory*, 34(5):1345–1348, 1988.

[35] H. Stichtenoth. *Algebraic Function Fields and Codes.* Springer, 1993.

[36] H. J. Tiersma. Remarks on codes from Hermitian curves. *IEEE Trans. Inform. Theory*, IT-33:605–609, 1987.

[37] M. A. Tsfasman, S. G. Vladut, and T. Zink. Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound. *Math. Nachr.*, 109:21–28, 1982.

[38] U. V. Vazirani. *Randomness, adversaries, and computation.* PhD thesis, EECS, UC Berkeley, 1986.