On bounding the number of rational places of function fields

Master's Thesis

Advanced Mathematical Topics with Applications

Kristian Skafte Jensen

Department of Mathematical Sciences

Aalborg University

AALBORG UNIVERSITY
STUDENT REPORT

Department of Mathematical Sciences
Skjernvej 4A
9220 Aalborg Øst
http://math.aau.dk

Title:
On bounding the number of rational places of function fields

Project Period:
Spring semester 2022

Student:

Kristian Skafte Jensen

Supervisor:
René Bødker Christensen

Page number: 51 (57 with appendices)
Finished: 3rd of June 2022

Synopsis:

The overall theme of this report is that of algebraic function fields. Specifically, we examine several bounds on the number of rational places of function fields over finite fields.
The necessary tools for discussing such bounds are introduced in the first chapter. This includes places, valuations, divisors and Riemann-Roch spaces. We also define Weierstraß semigroups and relate them to function fields. We then undertake the main task of the report by presenting and assessing five different bounds. Our point of departure is the Hasse-Weil bound, which is swiftly improved upon by Serre. We then assume further knowledge of our function field in order to examine the Lewittes and Geil-Matsumoto bound, the latter of which is further generalised by Beelen and Ruano.
Lastly, we apply the bounds on several families of function fields, for which we mention some of their known properties. We compare the results of the bounds for each function field by examples.

Preface

This report has been written as the master's thesis of Kristian Skafte Jensen during the spring semester of 2022 at the Department of Mathematical Sciences at Aalborg University. The main theme of the report is algebraic function fields. In this regard, the report describes several bounds on the number of rational places of function fields over finite constant fields.

The reader is assumed to be comfortable with abstract algebra as well as the basic principles of coding theory. Prerequisite knowledge of function fields is certainly beneficial, but the most essential of notions and results are presented in the first chapter of the report.

I would like to give many thanks to my supervisor René Bødker Christensen for the undying patience and for nearly always having answers to my questions readily available. I would also like to thank Matteo Bonini for helpful discussions regarding hyperelliptic curves.

Reading Guide

Throughout the report, we work with the convention $\mathbb{N} \coloneqq \{1, 2, 3, \ldots\}$ when referring to the natural numbers. When we want 0 to be included, we use the notion $\mathbb{N}_0 \coloneqq \mathbb{N} \cup \{0\}$. Furthermore, by $\mathbb{F}_q$ we denote the finite field of q elements, where $q = p^n$ with p prime and $n \in \mathbb{N}$. A more extensive, albeit not exhaustive list of commonly used notation in the report can be found in appendix C.

For referencing, in-text citation is denoted in author-year format, for instance [Stichtenoth, 2009], corresponding to an entry in the list of references. Definitions, theorems, propositions, lemmata, corollaries and examples are numbered on the form C.S.I, where C.S specifies the chapter and section, and I is the index. Likewise, equations are labelled on the form (C.I), where C specifies the chapter, and I is the index. Figures and tables are labelled similarly. Proofs are ended by the symbol $\square$, and examples are ended by the symbol $\triangleleft$.

Danish Abstract

Det overordnede tema for dette projekt er algebraiske funktionslegemer. Specifikt fokuseres der på diverse øvre grænser for antallet af rationale places for funktionslegemer med endelige konstantlegemer.

Projektets første kapitel gennemgår indledningsvist de nødvendige redskaber for at kunne beskrive de forskellige grænser. Dette indbefatter fundamentale definitioner af objekter såsom places, valueringer, divisorer og Riemann-Roch rum. To gentageligt anvendte resultater, Riemann-Roch sætningen og Weierstraß hulsætningen, præsenteres også i dette kapitel. Dernæst påbegyndes projektets hovedkapitel, hvori fem grænser for antallet af rationale places for funktionslegemer præsenteres. Udgangspunktet er Hasse-Weil grænsen, hvorfra forbedringer og generaliseringer følger. Vi introducerer maksimalitet og motiverer dennes relevans for kodningsteori. Undervejs motiveres grænserne med eksempler og sammenligninger af hinanden. Særligt sammenlignes Lewittes grænsen og Geil-Matsumoto grænsen, og det vises, hvornår disse grænser er ens.

I projektets sidste kapitel anvendes grænserne på specifikke familier af funktionslegemer. Heri præsenteres nogle kendte egenskaber for de forskellige funktionslegemer. Disse egenskaber bruges til at beregne øvre grænser for antallet af rationale places.

Contents

Introduction

In coding theory, a major interest lies in determining good parameters for different classes of codes. The method of pursuing these desirable parameters varies from class to class. One class of codes, whose parameters we examine in this report, is the class of algebraic geometry codes. A special case is the subclass of Reed-Solomon codes, in which the codewords are based on evaluations of polynomials. In general, algebraic geometry codes involves elements of algebraic function fields instead of polynomials, and these elements are evaluated in rational places of said function field. In terms of error-correction and efficient transmission, it is beneficial to acquire algebraic geometry codes of large length. One caveat of some codes, including Reed-Solomon codes, is that their length is bounded by the size of their field. Thus, codes of a desirable length require a large field. For general algebraic geometry codes, however, the length is determined by the number of rational places of the associated function field. This number is not exclusively determined by the field size, and so this allows for algebraic geometry codes with good parameters without the need for large fields.

In this thesis, we seek to present several different bounds on the number of rational places of algebraic function fields, which is supported by the necessary theory along the way. We will begin by a short summary of the tools required for further discussion of algebraic function fields. Some useful results that will be brought up on multiple occasions throughout the thesis are stated without proof. This includes the Riemann-Roch theorem and the Weierstraß gap theorem. We then mark the starting point of the study on bounds by showcasing the Hasse-Weil bound along with Serre's improvement for non-square field sizes. As these bounds are based on limited knowledge of the function field, we expand the theory by studying the Lewittes bound which also takes pole numbers of the function field into account. We show that this bound is stronger than the Serre bound for certain field sizes. Next, we generalise the Lewittes bound by examining a way to bound the number of rational places of a function field if is has a rational place with a specific Weierstraß semigroup. Known as the Geil-Matsumoto bound, we treat the case where the Weierstraß semigroup is generated by two integers, in which case we obtain a closed formula for the bound. We also compare it to the Lewittes bound and examine an upper bound on the field size for which the bounds can yields different values. Lastly, we further generalise by presenting a bound by Beelen and Ruano, which applies generalised Weierstraß semigroups. We argue that this is in fact a generalisation of

the Geil-Matsumoto bound.

In the final chapter, we apply the bounds presented on different classes of function fields for the purpose of comparing the strength of the bounds. For the cases where the exact numbers of rational places are known, we compare the bounds to these values.

The thesis is prepared by use of several papers as well as some textbooks that are popular in the literature. Some of the papers omit details, while others include minor oversights. An attempt is made to both fill in some missing details as well as avoid the same oversights.

CHAPTER 1

PRELIMINARIES

This chapter is based on [Stichtenoth, 2009]. In this chapter we give the basic definitions needed in order to discuss rational places of function fields. The results mentioned in this section are well-known, and most proofs are therefore not included. They will, however, be referred to when appropriate.

1.1 Function Fields

This first section is dedicated to the introduction of the most basic of tools needed for further discussion. We first introduce function fields, places and valuations. We then use these objects to define divisors and Riemann-Roch spaces. The section concludes with two results on the dimension of divisors, one of them being the Riemann-Roch theorem.

Definition 1.1.1:
*Let F/K be an extension field of K such that F is a finite algebraic extension of $K(x)$ where $x \in F$ is transcendental over K. Then F/K is called an **algebraic function field**. We define the **degree** of F/K, denoted $[F : K]$, as the dimension of F when considering F as a vector space over K.*

We always refer to an algebraic function field simply as a function field. Moreover, we will always assume that K, called the constant field of F, is algebraically closed in F. In other words, we assume that

$$K = \{z \in F : z \text{ is algebraic over } K\}.$$

Definition 1.1.2:
*Consider a function field F/K and let $\mathcal{O}$ be a ring such that $K \subsetneq \mathcal{O} \subsetneq F$ and if $z \in F$ then $z \in \mathcal{O}$ or $z \in \mathcal{O}^*$. Then $\mathcal{O}$ is called a **valuation ring**.*

*Let P denote the unique maximal ideal of $\mathcal{O}$ defined as $P = \mathcal{O} \setminus \mathcal{O}^*$. Then P is called a **place** of F/K. Additionally, we denote by $\mathbb{P}_F$ the set of all places of F/K.*

There is a close correspondence between places and valuation rings, see [Stichtenoth, 2009; Proposition 1.1.5]. Thus, we denote by $\mathcal{O}_P$ the valuation ring associated with the place P. Additionally, we can define a map that allows us to associate elements in F with places in $\mathbb{P}_F$, as described in the following definition.

Definition 1.1.3:
*For a function field F/K we define a **discrete valuation** by a map $v\colon F \to \mathbb{Z} \cup \{\infty\}$ that satisfies the following:*

i. $v(z) = \infty$ *if and only if* $z = 0$.
ii. $v(yz) = v(y) + v(z)$ *for all* $y, z \in F$.
iii. $v(y + z) \geq \min\{v(y), v(z)\}$ *for all* $y, z \in F$.
iv. There exists a $z \in F$ *such that* $v(z) = 1$.
v. $v(a) = 0$ *for all non-zero* $a \in K$.

A stricter version of point *iii.* in definition 1.1.3 can be derived in order to determine when we have an equality in $v(x + y) \geq \min\{v(x), v(y)\}$.

Proposition 1.1.4 (Strict Triangle Inequality):
Let v be a discrete valuation of a function field F/K, and let $x, y \in F$ such that $v(x) \neq v(y)$. Then $v(x + y) = \min\{v(x), v(y)\}$.

Proof. The proof follows more or less directly from definition 1.1.3. For non-zero $a \in K$, we have $v(ax) = v(a) + v(x) = v(x)$. Since clearly $-1 \in K$, we have the relation $v(-x) = v(x)$. Assume without loss of generality that $v(x) < v(y)$. Assume now for contradiction that $v(x + y) \neq \min\{v(x), v(y)\}$. Then by point *iii.* of definition 1.1.3, we must have $v(x + y) > v(x)$. We can then write $v(x) = v((x + y) - y) \geq \min\{v(x + y), v(y)\} > v(x)$; clearly a contradiction. □

Consider a place $P \in \mathbb{P}_F$. It can be shown that P is a principal ideal and that all non-zero elements $z \in F$ have the unique representation $z = t^n u$ where t is the generator of P, $n \in \mathbb{Z}$ and $u \in \mathcal{O}^*$, see [Stichtenoth, 2009; Theorem 1.1.6]. Then we define the discrete valuation of P $v_P\colon F \to \mathbb{Z} \cup \{\infty\}$ such that $v_P(z) \coloneqq n$ and $v_P(0) \coloneqq \infty$.

We emphasise the understanding of elements $z \in F$ being functions in the following. Consider $P \in \mathbb{P}_F$. Since P is a maximal ideal, we can define a field $F_P = \mathcal{O}_P/P$ which we call the residue class field of P. Now consider $z \in F$. If $z \in \mathcal{O}_P$ then we define $z(P) \in F_P$ to be the residue class of z modulo P, and if $z \notin \mathcal{O}_P$ we set $z(P) = \infty$. In this way we can regard elements in F as functions by way of the aforementioned construction. The places in $\mathbb{P}_F$ corresponds to points on which we can evaluate $z \in F$, and we say that $z(P)$ is z evaluated at P. We also introduce the notion of zeros and poles in a natural manner. We say that P is a zero of z if $z(P) = 0$ which by definition of $z(P)$ occurs when $z \in P$. Conversely, we say that P is a pole of z if $z(P) = \infty$ which by definition is equivalent to $z \notin \mathcal{O}_P$. Finally, we know that $K \subseteq \mathcal{O}_P$ and $K \cap P = \{0\}$ from [Stichtenoth, 2009; Proposition 1.1.5], so the residue class map $z \mapsto z(P)$ from $\mathcal{O}_P$ to F_P induces an embedding of K in F_P.

Definition 1.1.5:
*Let $P \in \mathbb{P}_F$. We define the **degree** of P as $\deg P \coloneqq [F_P : K]$. If $\deg P = 1$ we call P a **rational place**.*

We are interested in identifying elements $z \in F$ with a certain number of zeros and poles. For this purpose we will need divisors.

Definition 1.1.6:
*Let F/K be a function field. A **divisor** is a formal sum*

$$D = \sum_{P \in \mathbb{P}_F} n_P P,$$

*where $n_P \in \mathbb{Z}$ and with almost all $n_P = 0$. We denote by $\mathrm{Div}(F)$ the set of divisors of F. In fact, $\mathrm{Div}(F)$ is a group with component-wise addition, and as such we shall call $\mathrm{Div}(F)$ the **divisor group** of F. For $D \in \mathrm{Div}(F)$ we define $v_P(D) \coloneqq n_P$ and we define the support of D as $\mathrm{supp}(D) \coloneqq \{P \in \mathbb{P}_F | v_P(D) \neq 0\}$. We define a partial ordering of elements in $\mathrm{Div}(F)$ by means of the valuation map. For $D_1, D_2 \in \mathrm{Div}(F)$ we say that $D_1 \leq D_2$ if and only if $v_P(D_1) \leq v_P(D_2)$ for all $P \in \mathbb{P}_F$. We call a divisor D positive if $D \geq 0$. Lastly, we define the degree of $D \in \mathrm{Div}(F)$ by*

$$\deg D \coloneqq \sum_{P \in \mathbb{P}_F} v_P(D) \deg P.$$

Specifically, we are interested in certain types of divisors based on the zeros and poles of the elements in F.

Definition 1.1.7:
Let F/K be a function field and let $z \in F$ be non-zero. Let Z and N denote the sets of zeros and poles of z, respectively. Then the divisors

$$(z)_0 \coloneqq \sum_{P \in Z} v_P(z) P, \qquad (z)_\infty \coloneqq \sum_{P \in N} -v_P(z) P, \qquad (z) \coloneqq (z)_0 - (z)_\infty$$

*are called the **zero divisor**, the **pole divisor** and the **principal divisor** of z, respectively.*

Note that there are finitely many zeros and poles of any element $z \in F$, see [Stichtenoth, 2009; Corollary 1.3.4], thus definition 1.1.7 makes sense.

We are now ready to define Riemann-Roch spaces.

Definition 1.1.8:
Let F/K be a function field and let $D \in \mathrm{Div}(F)$. Then the set

$$\mathscr{L}(D) \coloneqq \{z \in F : (z) \geq -D\} \cup \{0\}$$

*is called the **Riemann-Roch space** associated to D.*

It is rather straightforward to show that $\mathscr{L}(D)$ is a K-vector space for any $D \in \mathrm{Div}(F)$, see for instance [Stichtenoth, 2009; Lemma 1.4.6]. Warranted by this fact, we define for any $D \in \mathrm{Div}(F)$ the *dimension* of D as $\ell(D) \coloneqq \dim(\mathscr{L}(D))$.

The following result show that all principal divisors are of degree 0. In essence this means that every non-zero $z \in F$ has an equal number of zeros and poles when counted properly, that is, when taking the degree of P as well as the valuation v_P into account.

Proposition 1.1.9:
Let $z \in F \setminus K$. Then

$$\deg(z)_0 = \deg(z)_\infty = [F : K(z)].$$

Proof. See [Stichtenoth, 2009; Theorem 1.4.11]. □

We now introduce an important invariant of Riemann-Roch spaces that is useful when we want to determine the dimension of divisors.

Definition 1.1.10:
Let F/K be a function field. Then

$$g \coloneqq \max_{D \in \mathrm{Div}(F)} \{\deg D - \ell(D) + 1\}$$

*is the **genus** of F.*

It can be shown that $\deg D - \ell(D)$ has an upper bound, see [Stichtenoth, 2009; Proposition 1.4.14], thus g is well-defined. Furthermore, by letting $D = 0$ we have $\deg 0 - \ell(0) + 1 = 0$, hence g is non-negative.

The following theorem allows us to determine the dimension of divisors. It is a consequence of the widely celebrated Riemann-Roch theorem.

Theorem 1.1.11 (Riemann-Roch):
Let F/K be a function field and let $D \in \mathrm{Div}(F)$. Then

$$\ell(D) \geq \deg D + 1 - g,$$

with equality when $\deg D \geq 2g - 1$.

In the thesis, we will invoke another result regarding the dimension of divisors, which is related to Weil differentials.

Definition 1.1.12:
*Let F/K be a function field. An **adele** is a map $\alpha \colon \mathbb{P}_F \to F$ given by $P \mapsto \alpha_P$ such that $v_P(\alpha_P) < 0$ for only a finite number of places. We denote*

$$\mathcal{A}_F \coloneqq \{\alpha : \alpha \text{ is an adele of } F/K\},$$
$$\mathcal{A}_F(D) \coloneqq \{\alpha \in \mathcal{A}_F : v_P(\alpha) \geq -v_P(D) \text{ for all } P \in \mathbb{P}_F\},$$

for $D \in \mathrm{Div}(F)$.

Definition 1.1.13:
*Let F/K be a function field and define a K-linear map $\omega \colon \mathcal{A}_F \to K$ such that $\omega(\mathcal{A}_F(D) + F) = 0$ for some $D \in \mathrm{Div}(F)$. Then ω is called a **Weil differential**. We denote*

$$\Omega_F \coloneqq \{\omega : \omega \text{ is a Weil differential of } F/K\},$$
$$\Omega_F(D) \coloneqq \{\omega \in \Omega_F : \omega(\mathcal{A}_F(D) + F) = 0\},$$

for $D \in \mathrm{Div}(F)$. Moreover, the divisor (ω) of the non-zero Weil differential $\omega \in \Omega_F$ is a divisor that satisfies $\omega(\mathcal{A}_F((\omega)) + F) = 0$ as well as $D \leq (\omega)$ for all $D \in \mathrm{Div}(F)$ where $\omega(\mathcal{A}_F(D) + F) = 0$.

Remark. In [Stichtenoth, 2009; Lemma 1.5.10] the existence and uniqueness of the divisor of a given Weil differential is shown, thus warranting the latter part of definition 1.1.13.

Definition 1.1.14:
Let $D \in \mathrm{Div}(F)$. Then

$$i(D) \coloneqq \ell(D) - \deg D + g - 1$$

*is called the **index of specialty** of D.*

Proposition 1.1.15:
For $D \in \mathrm{Div}(F)$ we have $\dim(\Omega_F(D)) = i(D)$.

Proof. See [Stichtenoth, 2009; Lemma 1.5.7]. □

Definition 1.1.14 and proposition 1.1.15 let us relate the dimension of a divisor to the dimension of the associated Weil differential space.

1.2 Weierstraß Semigroups

In the last part of this chapter, we introduce Weierstraß semigroups as they play a major role throughout the thesis.

Definition 1.2.1:
*Let F/K be a function field, let $n \in \mathbb{N}$ and let $P \in \mathbb{P}_F$ be rational. We then call n a **pole number** of P if there exists an element $z \in F$ such that $(z)_\infty = nP$. Otherwise, we call n a **gap number** of P.*

We show an upper bound on the gap numbers.

Proposition 1.2.2:
Let $P \in \mathbb{P}_F$. If $n \geq 2g$, then n is a pole number of P.

Proof. We have $\ell((n-1)P) = (n-1)\deg P + 1 - g$ and $\ell(nP) = n\deg P + 1 - g$ by the Riemann-Roch theorem 1.1.11 since $n \geq 2g - 1$. Therefore, $\mathscr{L}((n-1)P) \subsetneq \mathscr{L}(nP)$. Consider $z \in \mathscr{L}(nP) \setminus \mathscr{L}((n-1)P)$. If $z \notin \mathscr{L}((n-1)P)$ then either there exists other poles of z than P or $v_P(z) < -(n-1)$. The additional assumption that $z \in \mathscr{L}(nP)$ implies that $v_P(z) \geq -n$ and that P is the only pole of z. Thus, combining the two assumptions we have $v_P(z) = -n$ and $(z)_\infty = nP$, hence n is a pole number. □

We note that n is a pole number of P if and only if $\ell(nP) > \ell((n-1)P)$. Similarly, n is a gap number if and only if $\mathscr{L}(nP) = \mathscr{L}((n-1)P)$.

We denote by $H(P)$ the set of pole numbers of the place $P \in \mathbb{P}_F$. Clearly, $H(P) \subsetneq \mathbb{N}_0$ and moreover it is a sub-semigroup of $\mathbb{N}_0$ called the *Weierstraß semigroup* of P [Beelen et al., 2006]. The following theorem, known as the Weierstraß gap theorem, elaborates on the structure of Weierstraß semigroups.

Theorem 1.2.3 (Weierstraß Gap Theorem):
Let F/K be a function field of genus $g > 0$ and let $P \in \mathbb{P}_F$ be rational. Then there is exactly g gap numbers $i_1 < \cdots < i_g$ of P, where $i_1 = 1$ and $i_g \leq 2g - 1$.

Proof. See [Stichtenoth, 2009; Theorem 1.6.8]. □

Consider some rational place $P \in \mathbb{P}_F$ and its Weierstraß semigroup $H(P)$. Theorem 1.2.3 tells us that at least all $i > 2g - 1$ are in $H(P)$ along with 0. Moreover, there are $g - 1$ pole numbers in $[1, 2g-1]$. In fact, it is known that for almost all $P \in \mathbb{P}_F$ the set of gap numbers is the same. A place that has a different set of gaps is called a *Weierstraß point*. It can be shown that there can exist at most finitely many Weierstraß points, see for instance [Tsfasman et al., 1991; p. 165], and that if $g \geq 2$ then there exists at least one, see [Hirschfeld et al., 2013; p. 186].

Chapter 2

Bounds on Number of Rational Places

Consider a function field $F/\mathbb{F}_q$ over the finite field of q elements. Let $P_1, \ldots, P_n$ be pairwise distinct rational places of $F/\mathbb{F}_q$ and define a divisor $D = P_1 + \cdots + P_n$. Consider now another divisor $G \in \mathrm{Div}(F)$ such that $\mathrm{supp}(D) \cap \mathrm{supp}(G) = \varnothing$. Then the *algebraic geometry code*, or AG code, associated with D and G is defined as

$$\mathcal{C}_{\mathscr{L}}(D, G) \coloneqq \Big\{ \big(z(P_1), \ldots, z(P_n)\big) : z \in \mathscr{L}(G) \Big\} \subseteq \mathbb{F}_q^n.$$

Clearly, the length of $\mathcal{C}_{\mathscr{L}}(D, G)$ is n, the size of which is bounded by the number of rational places of $F/\mathbb{F}_q$. In the field of algebraic coding theory, it is therefore important to ask for a bound on the number of rational places of function fields. These bounds are mainly based on the alphabet size q, but we shall see that more information about the function field in question might lead to stronger bounds. At this time, the exact number of rational places is known for several function fields (see for instance [Geer et al., 2009]), however this is only true for $q = p^m$ where m is relatively small. Thus, finding good bounds is still an essential problem.

In the following chapter, we give a theoretical presentation of several bounds on the number of rational places of function fields over a finite field. Our starting point is the well-known Hasse-Weil bound. We hastily supply a slight improvement made by Serre and let this bound be our default bound for comparison. We then make the preparations in order to present a more recently proposed bound by Lewittes, which applies the knowledge of pole numbers of rational places. Next, we show a generalisation of Lewittes' bound by Geil and Matsumoto that bounds the number of rational places of any function field with a specific Weierstraß semigroup. Finally, as an additional generalisation, we present a bound by Beelen and Ruano that introduces the application of a generalisation of Weierstraß semigroups. Throughout the chapter, we make theoretical evaluations of the bounds as well as short examples, however a more thorough comparison will be saved for the next chapter.

We begin by introducing some useful notation. Letting F/K be a function field, we denote by $N(F)$ the number of rational places of F. When the function field is obvious from the context, we simply write $N \coloneqq N(F)$. Additionally, we will always assume that F/K is of genus g.

2.1 The Hasse-Weil and Serre Bounds

Our first two bounds determine the maximal number of rational places of a function field solely based on the field size and the genus. In particular, the first bound gives way for a notion of maximality for function fields. We show how this can be interpreted in coding theory.

2.1.1 The Hasse-Weil Bound

The Hasse-Weil bound will be our starting point for bounds on $N(F)$. This bound is derived directly from the Hasse-Weil theorem, and although the theory behind this result is immensely interesting in and of itself, it is quite extensive and not central for our purpose. We therefore simply present the bound as a point of departure for the following theory. The interested reader may find a reasonably pedagogical coverage of said theory in [Stichtenoth, 2009; Section 5.1].

Theorem 2.1.1 (Hasse-Weil Bound):
Let $F/\mathbb{F}_q$ be a function field. Then N satisfies

$$|N - (q+1)| \leq 2g\sqrt{q}.$$

Proof. See [Stichtenoth, 2009; Theorem 5.2.3]. □

Example 2.1.2:
Consider the so-called *Hermitian function field*, that is, $\mathbb{F}_{q^2}(x,y)/\mathbb{F}_{q^2}$ with $y^q + y = x^{q+1}$. Let $q = 4$, thus we have a function field over $\mathbb{F}_{16}$. It is known that the genus of the Hermitian function field is given by $g = \frac{q(q-1)}{2}$ [Stichtenoth, 2009; Lemma 6.4.4], thus $g = 6$. The Hasse-Weil bound yields

$$N \leq 2gq + q^2 + 1 = 2 \cdot 6 \cdot 4 + 16 + 1 = 65,$$

which is the exact number of rational places of the Hermitian function field, since another well-known fact is that is possesses exactly $q^3 + 1$ rational places. Therefore, this function field meets the Hasse-Weil bound. ◁

2.1.2 Maximality and Coding Theory

The notion of maximality for function fields has some qualities that are desirable in coding theory.

Definition 2.1.3:
*A function field $F/\mathbb{F}_q$ is called $\mathbb{F}_q$-**maximal** if $N(F) = 2g\sqrt{q} + q + 1$.*

Note that a function field can only be maximal if $g = 0$, or if q is a square.

One extensively studied maximal function field is the Hermitian function field. In this case, maximality is rather straightforward to verify.

Proposition 2.1.4:
Let $\mathcal{H}_q$ be the Hermitian function field over $\mathbb{F}_{q^2}$. Then $\mathcal{H}_q$ is $\mathbb{F}_{q^2}$-maximal.

Proof. From the Hasse-Weil bound we immediately obtain

$$\begin{aligned} N(\mathcal{H}_q) &\leq 2gq + q^2 + 1 \\ &= q(q-1)q + q^2 + 1 \\ &= q^3 - q^2 + q^2 + 1 \\ &= q^3 + 1, \end{aligned}$$

which we know to be exactly equal to $N(\mathcal{H}_q)$. □

We shall return to the Hermitian function fields later in the thesis.

We take a slight detour into the realm of coding theory. One nice property that maximal function fields deliver, when we wish to construct algebraic geometric codes, relates to the Singleton bound (see [Stichtenoth, 2009; Proposition 2.1.8]). It states that any $[n, k, d]$ code $\mathcal{C}$ satisfies $k + d \leq n + 1$. The theory of AG codes expand upon this with a lower bound (see [Stichtenoth, 2009; Theorem 2.2.2]). We thus have for any $[n, k, d]$ AG code that

$$n + 1 - g \leq k + d \leq n + 1. \tag{2.1}$$

This implies that the genus of the corresponding function field determines "how far" the code is from being an MDS code, that is, a code that attains the Singleton bound. Together with the fact that maximal function fields possess the maximum number of rational places with respect to their genus, equation (2.1) states that AG codes constructed from maximal function fields have the largest possible minimum distance with respect to their length and dimension. This has similar implications for asymptotically good codes as well. Two values of particular interest for an $[n, k, d]$ code is the information rate $R = \frac{k}{n}$ and the relative minimum distance $\delta = \frac{d}{n}$. These values are used to assess efficiency of codes both in terms of redundancy and error-correcting capabilities. Notice that from equation (2.1) we obtain

$$k + d \geq n + 1 - g \implies \frac{k+d}{n} \geq \frac{n+1-g}{n} \implies R + \delta \geq 1 - \frac{g-1}{n}.$$

We thus want g small and n large, and since n is directly determined by the number of rational places of the function field, this motivates another reason for our desire for many rational places [Høholdt et al., 1998; §2.9].

Furthermore, many examples of maximal function fields have large automorphism groups, which admit well-performing AG codes in that the codes inherit many symmetries [Bartoli et al., 2021a]. This has been shown to potentially lead to good performance in both encoding and decoding.

2.1.3 The Serre Bound

An improvement of the Hasse-Weil bound was remarked by Serre when q is not a square.

Theorem 2.1.5 (Serre Bound):
Let $F/\mathbb{F}_q$ be a function field. Then N satisfies

$$|N - (q+1)| \leq g\lfloor 2\sqrt{q} \rfloor.$$

Proof. See [Serre, 1983; Theorem 1]. □

Theorem 2.1.5 directly implies an upper bound on N of the form

$$N \leq g\lfloor 2\sqrt{q} \rfloor + q + 1,$$

which shall be our reference point when presenting other bounds.

2.2 The Lewittes Bound

Based on [Lewittes, 1990], this section attempts to formulate a bound that improves upon the Serre bound by applying more information about the function field. Specifically, we show a bound on $N(F)$ that depends on a pole number of some rational place of F/K. In order to obtain this bound, however, we shall begin by introducing algebraic extensions of function fields.

Definition 2.2.1:
*Let F/K and F'/K' be function fields. If $F' \supseteq F$ is an algebraic field extension and $K' \supseteq K$, then F'/K' is called an **algebraic extension** of F/K.*

We say that the algebraic extension F'/K' is finite if $[F' : F] < \infty$.

Next we consider places of algebraic extensions of function fields and their relation to the places of the underlying function field.

Definition 2.2.2:
*Let F'/K' be an algebraic extension of F/K. We say that a place $P' \in \mathbb{P}_{F'}$ **lies over** $P \in \mathbb{P}_F$ if $P \subseteq P'$. Equivalently, we say that P **lies under** P', and we denote the relation by $P'|P$.*

Proposition 2.2.3:
Let F'/K' be an algebraic extension of F/K, and let $P \in \mathbb{P}_F$ and $P' \in \mathbb{P}_{F'}$. Then P' lies over P if and only if there exists some integer $e \geq 1$ such that $v_{P'}(z) = e \cdot v_P(z)$ for all $z \in F$.

Proof. We claim that P' lies over P if and only if $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$. The proof of this claim can be found in [Stichtenoth, 2009; Proposition 3.1.4]. We now show that there exists an $e \geq 1$ such that $v_{P'}(z) = e \cdot v_P(z)$ if and only if $\mathcal{O}_P \subseteq \mathcal{O}_{P'}$. Let us first assume the latter. Let $y \in F$

such that $v_P(y) = 0$. Then $y, y^{-1} \in \mathcal{O}_P$ and hence they are also contained in $\mathcal{O}_{P'}$ by our assumption. We therefore also have $v_{P'}(y) = 0$. Choose now $t \in F$ such that $v_P(t) = 1$ and define $e \coloneqq v_{P'}(t)$. Since P lies under P' by our initial claim, it must hold that $e \geq 1$. Now choose a non-zero $z \in F$ and denote $r \coloneqq v_P(z)$. Then we have $v_P(zt^{-r}) = v_P(z) + v_P(t^{-r}) = r - r = 0$, and for P' we obtain

$$v_{P'}(z) = v_{P'}(zt^r t^{-r}) = v_{P'}(zt^{-r}) + v_{P'}(t^r) = 0 + r \cdot v_{P'}(t) = e \cdot v_P(z).$$

For the converse, assume that $v_{P'}(z) = e \cdot v_P(z)$ for some $z \in F$ and some $e \geq 1$. Now assume that $z \in \mathcal{O}_P$. This implies that $v_P(z) \geq 0$, thus $v_{P'}(z) = e \cdot v_P(z) \geq 0$ so $z \in \mathcal{O}_{P'}$ as well. By our initial claim, this completes the proof. □

Proposition 2.2.3 leads to the following important notion.

Definition 2.2.4:
Let F'/K' be an algebraic extension of F/K and let $P'|P$ for some $P' \in \mathbb{P}_{F'}$ and $P \in \mathbb{P}_F$. The integer $e(P'|P)$ that satisfies

$$v_{P'}(z) = e(P'|P) \cdot v_P(z)$$

*for all $z \in F$ is called the **ramification index** of P' over P.*
*Additionally, we call $f(P'|P) \coloneqq [F'_{P'} : F_P]$ the **relative degree** of P' over P.*

Remark. Notice that $f(P'|P)$ can be finite or infinite, and it is finite if and only if F'/K' is finite [Stichtenoth, 2009; Proposition 3.1.6].

Lemma 2.2.5:
Let F'/K' be an algebraic extension of F/K and let $P' \in \mathbb{P}_{F'}$. Then there exists a non-zero $z \in F$ such that $v_{P'}(z) \neq 0$.

Proof. Assume for contradiction that such an element does not exist. We now choose $\zeta \in F'$ such that $v_{P'}(\zeta) > 0$. Such an element must necessarily exist, since otherwise $P' = \varnothing$ which would not be a place. Now, since F'/F is an algebraic field extension, ζ satisfies the equation

$$c_n\zeta^n + c_{n-1}\zeta^{n-1} + \cdots + c_1\zeta + c_0 = 0, \tag{2.2}$$

where $c_i \in F$ and $c_n \neq 0 \neq c_0$. By assumption $v_{P'}(c_0) = 0$ and by the properties of valuations we have $v_{P'}(c_i\zeta^i) = v_{P'}(c_i) + iv_{P'}(\zeta) > 0$ for $i = 1, \ldots, n$. Since the expression in (2.2) equals 0, we also have $v_{P'}(c_n\zeta^n + c_{n-1}\zeta^{n-1} + \cdots + c_1\zeta + c_0) = \infty$. This is a contradiction to the Strict Triangle Inequality, see proposition 1.1.4, hence there must exist $z \in F$ with $v_{P'}(z) \neq 0$. □

Proposition 2.2.6:
Let F'/K' be an algebraic extension of F/K. For each $P' \in \mathbb{P}_{F'}$ there exists exactly one $P \in \mathbb{P}_F$ such that $P'|P$, given by $P = P' \cap F$.

Proof. Let $P = P' \cap F$ and $\mathcal{O} \coloneqq \mathcal{O}_{P'} \cap F$. Then by lemma 2.2.5 $\mathcal{O}$ is a valuation ring of F/K, and P is the associated place. To prove uniqueness, let $Q \in \mathbb{P}_F$ and assume that $P'|Q$. Then by definition $Q \subseteq P'$ and we also have $Q \subseteq F$ since $Q \in \mathbb{P}_F$. Thus, $Q \subseteq P' \cap F = P$. The converse inclusion follows since both Q and P' are maximal ideals. □

Proposition 2.2.7:
Let F'/K' be an algebraic extension of F/K. Then every $P \in \mathbb{P}_F$ has at least one, but only finitely many extensions $P' \in \mathbb{P}_{F'}$.

Proof. Let $P \in \mathbb{P}_F$. Choose now a $z \in F \setminus K$ whose only zero is P. We can do this due to proposition 1.2.2 which guarantees the existence of an element with a single pole. Clearly, the inverse will then have a single zero. We first show that $P'|P$ if and only if $v_{P'}(z) > 0$ for $P' \in \mathbb{P}_{F'}$. If $P'|P$, then $v_{P'}(z) = e(P'|P) \cdot v_P(z) > 0$ since $z \in P$ by assumption. Conversely, we assume that $v_{P'}(z) > 0$ and let $Q \in \mathbb{P}_F$ such that $P'|Q$, the existence of which is warranted by proposition 2.2.6. Then $v_Q(z) > 0$ but this implies that $Q = P$ since P is the only zero of z in F/K. Now since z has at least one zero in F'/K', namely P', but only finitely many, then by the proven equivalence P has at least one but only finitely many extensions. □

Lemma 2.2.8:
Let K'/K be a finite field extension and let x be transcendental over K. Then

$$[K'(x) : K(x)] = [K' : K].$$

Proof. We can assume that K' is a simple extension of K, that is, $K' = K(\alpha)$ for some $\alpha \in K'$. In the general case we then just work our way through the intermediate fields between K and K' and split $[K' : K]$ into $[K' : K_1] \cdot [K_1 : K_2] \cdots [K_m : K]$ and use the base case on each step.

We begin by showing that $[K'(x) : K(x)] \leq [K' : K]$. To do this, we show that a basis for K' over K always span $K'(x)$ over $K(x)$. Thus, let $\{x^i\}_i$ be a basis for $K'(x)$ over $K(x)$ and let $y \in K'(x)$. Then we can write $y = \sum_i u_i x^i$ with $u_i \in K'$. Now let $\{z_j\}_j$ be a basis for K' over K. Then we can express u_i in this basis as $u_i = \sum_j v_{ij} z_j$ with $v_{ij} \in K$. Then we have

$$y = \sum_i \sum_j v_{ij} z_j x^i = \sum_j w_j z_j$$

with $w_j \in K(x)$.

To show the other direction, we use that $[K(\alpha) : K] = \deg \varrho$ where ϱ is the minimal polynomial of α over K [Brzeziński, 2018; Theorem 4.2]. We then want to show that ϱ is the minimal polynomial of α over $K(x)$ as well. Suppose for contradiction that this is not the case, such that $\varrho(T) = g(T) \cdot h(T)$ with $g, h \in K(x)[T]$ monic and both of degree smaller

than $\deg \varrho$. Since ϱ is the minimal polynomial of α it holds that $\varrho(\alpha) = 0$, so assume without loss of generality that $g(\alpha) = 0$. Thus, denoting $\deg g = d > 0$, we have

$$g(\alpha) = \alpha^d + f_{d-1}(x)\alpha^{d-1} + \cdots + f_0(x) = 0,$$

with $f_i(x) \in K(x)$. We can multiply by a common denominator of the $f_i(x)$ to obtain

$$g_d(x)\alpha^d + g_{d-1}(x)\alpha^{d-1} + \cdots + g_0(x) = 0. \tag{2.3}$$

Clearly, the left hand side of (2.3) is in $K[x][\alpha]$, however we can consider it as being in $K(\alpha)[x] = K'[x]$ as well by the corresponding equation

$$l_s(\alpha)x^s + l_{s-1}(\alpha)x^{s-1} + \cdots + f_0(\alpha) = 0, \tag{2.4}$$

with $l_j(\alpha) \in K(\alpha)$. Furthermore, we can assume that not all $g_i(x)$ in (2.3) are divisible by x. This means that there is a term $g_i(x)\alpha^i$ in which no x is present, which must then be a part of the constant term $l_0(\alpha) \in K(\alpha)$ when considering (2.3) as in (2.4). Now, since x is transcendental over K, all the $l_i(\alpha)$ must be zero. If they were not, then equation (2.4) would lead to a contradiction. In particular, we have $l_0(\alpha) = 0$ so $l_0 \in K[T]$ is of smaller degree than ϱ, which contradicts the minimality of ϱ over K. □

Theorem 2.2.9 (Fundamental Equality):
Let F'/K' be a finite extension of F/K. Let $P \in \mathbb{P}_F$ and let $P_1, \ldots, P_m \in \mathbb{P}_{F'}$ be all lying over P. Let $e_i \coloneqq e(P_i|P)$ and $f_i \coloneqq f(P_i|P)$, and let $n \coloneqq [F' : F]$. Then

$$\sum_{i=1}^{m} e_i f_i = n.$$

Proof. We begin by letting $z \in F$ be chosen such that P is the only zero of z in F/K and denoting $r \coloneqq v_P(z) > 0$. Then by the proof of proposition 2.2.7, the places $P_1 \ldots, P_m$ are exactly the zeros of z in F'/K'. Evaluating the degree of F' over $K(z)$, we obtain

$$\begin{aligned}
[F' : K(z)] &= [F' : K'(z)] \cdot [K'(z) : K(z)] \\
&= \left(\sum_{i=1}^{m} v_{P_i}(z) \deg P_i \right) \cdot [K' : K] \\
&= \left(\sum_{i=1}^{m} e_i \cdot v_P(z) \cdot [F'_{P_i} : K'] \right) \cdot [K' : K] \\
&= r \cdot \sum_{i=1}^{m} e_i \cdot [F'_{P_i} : F_P] \cdot [F_P : K] \\
&= r \cdot \deg P \cdot \sum_{i=1}^{m} e_i f_i.
\end{aligned} \tag{2.5}$$

The first equality is due to the Tower Law. The second equality follows from proposition 1.1.9 and lemma 2.2.8. For the third equality we simply use the definitions of e_i and $\deg P_i$, and in the fourth we exchange K' with F_P as the Tower Law declares the products equal.

We can, however, evaluate $[F' : K(z)]$ in another way

$$[F' : K(z)] = n \cdot [F : K(z)] = n \cdot r \cdot \deg P, \tag{2.6}$$

once again using proposition 1.1.9 and the fact that $(z)_0 = rP$. Finally, by comparing (2.5) and (2.6), we obtain the desired result. □

Consider a function field $F'/\mathbb{F}_q$ and let F be a subfield of F' such that $F/\mathbb{F}_q$ is a function field as well. For $P \in \mathbb{P}_F$ and $P' \in \mathbb{P}_{F'}$ we have

$$f(P'|P) \cdot \deg P = [F'_{P'} : F_P] \cdot [F_P : \mathbb{F}_q] = [F'_{P'} : \mathbb{F}_q] = \deg P'.$$

Thus, P' is rational if and only if P is rational and $f(P'|P) = 1$. In general, because we have $f(P'|P) > 0$, it holds that $\deg P' > \deg P$, so rational places of F' always lie over rational places of F.

Consider now some $P \in \mathbb{P}_F$. We define

$$m(P) \coloneqq \left| \left\{ P' \in \mathbb{P}_{F'} \colon P' | P, f(P'|P) = 1 \right\} \right|,$$

and let $n = [F' : F]$ as in theorem 2.2.9. By this notion, we sum over the rational places of F to obtain the bound

$$N(F') = \sum_P m(P) \leq N(F)n. \tag{2.7}$$

To see how we obtain the inequality, recall from theorem 2.2.9 that for each $P \in \mathbb{P}_F$, we have $\sum e(P_i|P)f(P_i|P) = n$, where we are summing over the finite number of places that lie over P. Since both $e(P_i|P)$ and $f(P_i|P)$ are positive integers, we have at most n terms in the sum, implying that there are at most n places lying over P. Since $m(P)$ is bounded by the number of places lying over P, the inequality follows.

To exemplify the application of (2.7), consider the function field $F/\mathbb{F}_q(x)$ where $x \in F \setminus \mathbb{F}_q$. By [Stichtenoth, 2009; Corollary 1.2.3] we have exactly $q + 1$ rational places of $\mathbb{F}_q(x)$. The first q of them are of the form

$$P_\alpha \coloneqq \left\{ \frac{f(x)}{g(x)} \colon f(x), g(x) \in \mathbb{F}_q[x], p(x) | f(x), p(x) \nmid g(x) \right\},$$

where $p(x) = x - \alpha$ for $\alpha \in \mathbb{F}_q$. The last rational place of $\mathbb{F}_q(x)$ is the so called place at infinity of $\mathbb{F}_q(x)$, P_∞. We have $n = [F : \mathbb{F}_q(x)] = \deg (x)_\infty$ by proposition 1.1.9. Thus, (2.7) yields

$$N \leq (q + 1) \deg (x)_\infty.$$

This expression vaguely resembles what we shall come to call Lewittes' bound. For us to get there, we need the following lemma.

Lemma 2.2.10:
Let F/K be a function field of genus g and assume that $N \geq 1$. Then there exists $z \in F \setminus K$ such that $[F : K(z)] \leq g$ and $m(P_\infty) \leq 2$, where P_∞ denotes the infinite place of $K(z)$.

Proof. We begin by considering the rational place $P \in \mathbb{P}_F$. Consider the positive divisor $D = (g-1)P$. Since $D \geq 0$ we have $K = \mathscr{L}(0) \subseteq \mathscr{L}(D)$ so $\ell(D) \geq 1$. This implies that

$$i(D) \coloneqq \ell(D) - \deg D + g - 1 \geq g - \deg D,$$

and since $\deg D = g-1$ we thus have $i(D) \geq 1$. Now let $\omega \in \Omega_F(D)$ such that $(\omega) = D + A$, where A is positive with $\deg A = g - 1$ since by [Stichtenoth, 2009; Corollary 1.5.16] we have $\deg(\omega) = 2g - 2$. We now pick a place Q contained in A and denote $\deg Q = d$. Define the divisor $B = (g-d)P + Q$, thus clearly $\deg B = g$ and moreover we have

$$B + (A - Q + (d-1)P) = (g-d)P + Q + (A - Q + (d-1)P) = (g-1)P + A = (\omega).$$

Since $A - Q \geq 0$ we thus have $(\omega) \geq B$ so $i(B) \geq 1$ by proposition 1.1.15. By this we obtain $\ell(B) \geq 2$ so there exists $z \in F \setminus K$ such that $(z) = (z)_0 - (z)_\infty \geq -B$ for all $P \in \mathbb{P}_F$, which means that $B + (z)_0 \geq (z)_\infty$. Notice that by definition $\operatorname{supp}((z)_0) \cap \operatorname{supp}((z)_\infty) = \varnothing$. Thus, for $P \in \operatorname{supp}((x)_\infty)$, subtracting $(z)_0$ does not disturb the inequality $B \geq (z)_\infty$. Furthermore, for $P \notin \operatorname{supp}((z)_\infty)$ we obviously have $v_P((z)_\infty) = 0$ and since $B \geq 0$ by assumption, it generally holds that $B \geq (z)_\infty$. Thus, by proposition 1.1.9, we have that $[F : K(z)] = \deg(z)_\infty \leq \deg B = g$.

For the second part, recall that P_∞ is the only pole of z in $K(z)$. Since all extensions $P|P_\infty$ satisfy

$$v_P(z) = e(P|P_\infty) v_{P_\infty}(z),$$

where $e(P|P_\infty) > 0$ and $v_{P_\infty}(z) < 0$, we have consequently that all rational places that lie over P_∞ must be poles of z in $\mathbb{P}_F$ and must therefore be contained in $(z)_\infty$. Thus, $m(P_\infty)$ is the number of rational places contained in $(z)_\infty$ which is bounded by the number of rational places contained in B. Since $B = (g-d)P + Q$, this is at most 2, hence $m(P_\infty) \leq 2$. □

We are now prepared to formulate the Lewittes bound.

Theorem 2.2.11 (Lewittes Bound):
Let $F/\mathbb{F}_q$ be a function field of genus $g \geq 2$. Then

$$N \leq qg + 2. \tag{2.8}$$

Furthermore, if $P \in \mathbb{P}_F$ is rational and $n \in H(P)$ then

$$N \leq qn + 1. \tag{2.9}$$

Proof. For the first part, we apply lemma 2.2.10 which guarantees the existence of $z \in F$ such that $[F : K(z)] \leq g$ and $m(P_\infty) \leq 2$. Then by equation (2.7) we obtain

$$N = \sum_{\alpha \in \mathbb{F}_q} m(P_\alpha) + m(P_\infty) \leq qn + 2 \leq qg + 2.$$

For the second part, we recall that if $n \in H(P)$ for some $P \in \mathbb{P}_F$, then there is a $z \in F$ such that $(z)_\infty = nP$. Recall that $m(P_\infty)$ is the number of rational places contained in $(z)_\infty$. Since $(z)_\infty = nP$, we thus have $m(P_\infty) = 1$, so (2.9) follows from the above inequality. □

To see when the Lewittes bound is guaranteed to be stronger than the Serre bound, consider the cases where $q = 2, 3, 4$. Recall that the Serre bound implies that $N \leq g\lfloor 2\sqrt{q} \rfloor + q + 1$. Notice that $\lfloor 2\sqrt{q} \rfloor = q$ in these cases, which implies

$$N \leq qg + 2 < qg + q + 1 = g\lfloor 2\sqrt{q} \rfloor + q + 1.$$

Thus the Lewittes bound is stronger than the Serre bound in these cases.

Example 2.2.12:
Consider a function field $F/\mathbb{F}_q$ of genus $g = 2$. In his tables, Serre has shown the exact number of rational places for several values of q, seen in table 2.1.

q	2	3	4	5	7	8	9	11	13
N	6	8	10	12	16	18	20	24	26

Table 2.1: The number of rational places of $F/\mathbb{F}_q$ with $g = 2$ as calculated in [Serre, 1982].

Notice that for $q \leq 11$, N attains the Lewittes bound of $N \leq 2q + 2$. Thus, for $g = 2$ and $q \leq 11$, this bound is strict. ◁

To clarify, we are most often interested in the bound given in equation (2.9). As such, this is what we usually refer to when mentioning the Lewittes bound. Notice also that we in (2.9) just require that $n \in H(P)$. Thus, it always makes sense to choose the smallest non-zero element in $H(P)$. We will see this again when deriving the Lewittes bound as a special case of the bound presented in the following section.

2.3 The Geil-Matsumoto Bound

So far, the bounds we have examined only let us dictate the cardinality q of the constant field and the genus g of the function field. In the following, we derive a bound, originally proposed in [Geil et al., 2009], that let us inspect function fields with a rational place having a certain Weierstraß semigroup. As we shall see, this bound yields a significant improvement to the previous bounds in some cases.

For the remainder of the report, we denote by Λ a finite sub-monoid of $\mathbb{N}_0$, where the set $\{\lambda_1, \ldots, \lambda_m\}$ is a generating set of Λ such that $0 < \lambda_1 < \cdots < \lambda_m$. This is known as a *numerical semigroup*. Supported by the Weierstraß Gap Theorem 1.2.3, we say that a numerical semigroup Λ is of genus g if it has g gaps, that is, if $|\mathbb{N}_0 \setminus \Lambda| = g$. We also use the notation $\alpha + \Lambda \coloneqq \{\alpha + \lambda : \lambda \in \Lambda\}$.

Definition 2.3.1:
Let Λ be fixed. If there exist function fields $F/\mathbb{F}_q$ with a rational place P such that $H(P) = \Lambda$, then we define $N_q(\Lambda)$ to be the largest possible number of rational places of any such function field, that is

$$N_q(\Lambda) \coloneqq \max\{N(F) \,:\, F/\mathbb{F}_q \text{ is a function field with a rational place } P \text{ such that } H(P) = \Lambda\}.$$

If no such function field exists, then we define $N_q(\Lambda) \coloneqq 0$.

The Geil-Matsumoto bound is an upper bound on $N_q(\Lambda)$. It is thus not only a bound on the number of rational places for function fields with some fixed q, but instead a bound on the number of rational places for any function field that has a rational place with Λ as their Weierstraß semigroup.

Theorem 2.3.2 (Geil-Matsumoto bound):
Let Λ be fixed. Then $N_q(\Lambda)$ satisfies

$$N_q(\Lambda) \leq \left| \Lambda \setminus \bigcup_{i=1}^{m} (q\lambda_i + \Lambda) \right| + 1. \tag{2.10}$$

Proof. Consider some function field $F/\mathbb{F}_q$ with rational places $P_1, \ldots, P_{N-1}, P \in \mathbb{P}_F$ and assume that $H(P) = \Lambda$ for a fixed Λ. Recall for any $t \in \mathbb{N}_0$ that

$$\begin{aligned} t \in \Lambda &\iff \ell(tP) = \ell((t-1)P) + 1, \\ t \notin \Lambda &\iff \mathscr{L}(tP) = \mathscr{L}((t-1)P). \end{aligned} \tag{2.11}$$

Define the space $\mathscr{L} = \bigcup_{r=0}^{\infty} \mathscr{L}(rP)$ and let an evaluation map $\mathrm{ev}\colon \mathscr{L} \to \mathbb{F}_q^{N-1}$ be given by $z \mapsto (z(P_1), \ldots, z(P_{N-1}))$. Define now $\mathcal{E}_t \coloneqq \mathrm{ev}(\mathscr{L}(tP))$ for $t \in \mathbb{N}_0 \cup \{-1\}$. By equation (2.11) we now have $\dim(\mathcal{E}_{-1}) = 0$ since $\mathscr{L}(-P) = \{0\}$, and we have $\dim(\mathcal{E}_t) = \dim(\mathcal{E}_{t-1})$ for $t \in \mathbb{N}_0 \setminus \Lambda$, since clearly $\mathcal{E}_t = \mathcal{E}_{t-1}$ when $\mathscr{L}(tP) = \mathscr{L}((t-1)P)$. On the other hand, consider the case where $t \in \Lambda$. Let $\mathcal{B} \coloneqq \{z_1, \ldots, z_m\}$ be a basis for $\mathscr{L}((t-1)P)$ and suppose $\mathrm{ev}(z) \in \mathcal{E}_{t-1}$ for some $z \in \mathscr{L}((t-1)P)$. Then we can write

$$\mathrm{ev}(z) = \mathrm{ev}(c_1 z_1 + \cdots + c_m z_m) = c_1 \mathrm{ev}(z_1) + \cdots + c_m \mathrm{ev}(z_m)$$

due to the linearity of ev. Thus, $\mathrm{span}\{\mathrm{ev}(z_1), \ldots, \mathrm{ev}(z_m)\} = \mathcal{E}_{t-1}$. Now consider the extension $\mathcal{B}^* = \mathcal{B} \cup \{y\}$ with $y \in \mathscr{L}(tP)$. Then $\mathcal{B}^*$ is a basis for $\mathscr{L}(tP)$ and $\mathrm{ev}(\mathcal{B}^*)$ spans $\mathcal{E}_t$. Now

$\dim(\mathcal{E}_t) = \dim(\mathcal{E}_{t-1})$ if $\mathrm{ev}(y)$ is linearly dependent on $\mathrm{ev}(B)$, and $\dim(\mathcal{E}_t) = \dim(\mathcal{E}_{t-1}) + 1$ if it is linearly independent.

Notice that we have defined $\mathcal{E}_t$ to be the algebraic geometry code $\mathcal{C}_{\mathscr{L}}(D, G)$ where $D = P_1 + P_2 + \cdots + P_{N-1}$ and $G = tP$. It is known that $\dim(\mathcal{C}_{\mathscr{L}}(D, G)) = \ell(G) - \ell(G - D)$, see for instance [Stichtenoth, 2009; Theorem 2.2.2]. Furthermore, by theorem 1.1.11 we have $\ell(D) = \deg D - g + 1$ for any $D \in \mathrm{Div}(F)$ with $\deg D$ sufficiently large. We now obtain

$$\begin{aligned}\dim(\mathcal{E}_t) &= \ell(G) - \ell(G - D) \\ &= (t - g + 1) - (t - (N - 1) - g + 1) \\ &= N - 1,\end{aligned}$$

for t sufficiently large. We want to know at what point this occurs, as this leads to the Geil-Matsumoto bound. To see why, consider the codes $\mathcal{E}_{-1}, \mathcal{E}_0, \mathcal{E}_1, \ldots$. We know that $\dim(\mathcal{E}_{-1}) = 0$ and that for some $t^* \in \Lambda$ sufficiently large, $\dim(\mathcal{E}_{t^*}) = N-1$. Furthermore, we have just seen that for the dimension to increase, we must have $t \in \Lambda$ in which case $\ell(tP) = \ell((t-1)P)+1$. Now, if we can show that elements $t \in \Lambda$ of a certain form does never increase the dimension, we can remove them from Λ, our initial set of candidates for increasing the dimension. We are then left only with the elements that might increase the dimension, the number of which must be at least $N-1$. We thus need to show that elements that never increase the dimension can be expressed as $q\lambda_i + \Lambda$. In other words, we wish to show that $\dim(\mathcal{E}_t) = \dim(\mathcal{E}_{t-1}) + 1$ only occurs when $t \neq q\lambda_i + \lambda$ for any $i = 1, 2, \ldots, m$ and any $\lambda \in \Lambda$.

We now let $z_i \in \mathscr{L}$ such that $v_P(z_i) = -\lambda_i$ for $i = 1, 2, \ldots, m$. Let $t = q\lambda_i + \lambda$ for some $\lambda \in \Lambda$ and choose $y \in \mathscr{L}(\lambda P) \setminus \mathscr{L}((\lambda - 1)P)$, which implies that $v_P(y) = -\lambda$. We obtain

$$v_P(z_i^q y) = q v_P(z_i) + v_P(y) = -(q\lambda_i + \lambda) = -t,$$

hence $z_i^q y \in \mathscr{L}(tP) \setminus \mathscr{L}((t-1)P)$. Similarly, we have

$$v_P(z_i y) = v_P(z_i) + v_P(y) = -(\lambda_i + \lambda) \geq -(t-1)$$

so $z_i y \in \mathscr{L}((t-1)P)$. Finally, we have

$$\mathrm{ev}(z_i^q y)_k = (z_i^q y)(P_k) = (z_i)(P_k)^q \cdot y(P_k) = (z_i)(P_k) \cdot y(P_K) = \mathrm{ev}(z_i y)_k$$

for $k = 1, \ldots, N-1$. Thus the new basis element in $\mathscr{L}(tP)$ evaluates to the same value as an element in $\mathscr{L}((t-1)P)$. This means that $\dim(\mathcal{E}_t)$ does not increase when $t = q\lambda_i + \lambda$, so removing all elements of this form from Λ will leave at least $N-1$ elements behind, which concludes the proof. □

We give an example of applying the Geil-Matsumoto bound with a certain semigroup. This specific semigroup is obtained from [COS++, 2021], but one can generate numerical semigroups for any given genus g recursively by the brute-force method presented in [Bras-Amorós, 2008].

Example 2.3.3:
Consider the generating set $\{7, 10, 13, 18\}$. This set generates the numerical semigroup

$$\Lambda = \{0, 7, 10, 13, 14, 17, 18, 20, 21, 23, 24, 25, 26, 27, 28\} \cup \{i \in \mathbb{N}_0 \colon i \geq 30\},$$

of genus $g = 15$. Assume that there exists some function field $F/\mathbb{F}_q$ with $q = 2$ and with a rational place that has Weierstraß semigroup equal to Λ. Then from the Geil-Matsumoto bound we obtain $N_2(\Lambda) \leq 9$. In comparison, the Serre bound yields $N(F) \leq 33$. Thus, if the Weierstraß semigroup is known for a rational place of the function field, the Geil-Matsumoto bound yields a drastically stronger upper bound in this case. ◁

The following result, the proof of which can be found in [Høholdt et al., 1998; Lemma 5.15], proves useful when we want to examine a special case of theorem 2.3.2.

Proposition 2.3.4:
Let Λ be fixed and let $\lambda \in \Lambda$. Then $|\Lambda \setminus (\lambda + \Lambda)| = \lambda$.

Proof. Let $c \in \Lambda$ be the smallest number such that $\{n \in \mathbb{N}_0 : n \geq c\} \subseteq \Lambda$, and define $\mathcal{T} \coloneqq \{t \in \mathbb{N}_0 : t \geq \lambda + c\}$. Then we have both $\mathcal{T} \subseteq \Lambda$ and $\mathcal{T} \subseteq \lambda + \Lambda$. Now define $\mathcal{U} \coloneqq \{u \in \Lambda : u < \lambda + c\}$. By theorem 1.2.3 we know that $|\mathbb{N}_0 \setminus \Lambda| = g$, implying that $|\mathcal{U}| = \lambda + c - g$. Thus, $\mathcal{T}$ and $\mathcal{U}$ form a partition of Λ. Define $\mathcal{V} \coloneqq \{v \in \lambda + \Lambda : \lambda \leq v < \lambda + c\}$. Clearly $|\mathcal{V}| = c - g$, and $\mathcal{V}$ and $\mathcal{T}$ form a partition of $\lambda + \Lambda$. Since $\lambda \in \Lambda$ and Λ is a semigroup, we have $\lambda + \Lambda \subseteq \Lambda$, thus $\mathcal{V} \subseteq \mathcal{U}$. An illustration showcasing the sets in relation to each other can be seen in figure 2.1.

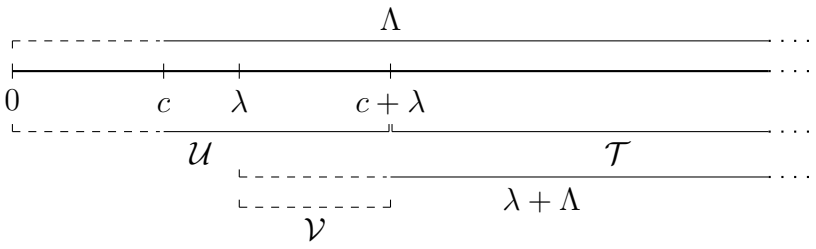

Figure 2.1: Visual representation of sets with dashed lines representing the g gaps not included in Λ.

Finally, we obtain

$$\begin{aligned} |\Lambda \setminus (\lambda + \Lambda)| &= |(\mathcal{U} \cup \mathcal{T}) \setminus (\mathcal{V} \cup \mathcal{T})| \\ &= |\mathcal{U} \setminus \mathcal{V}| \\ &= |\mathcal{U}| - |\mathcal{V}| \\ &= (\lambda + c - g) - (c - g) \\ &= \lambda, \end{aligned}$$

as desired. □

Next, we show that one can obtain the Lewittes bound from the Geil-Matsumoto bound.

Corollary 2.3.5:
Let Λ be fixed. Then $N_q(\Lambda)$ satisfies

$$N_q(\Lambda) \leq q\lambda_1 + 1. \tag{2.12}$$

Proof. We have directly from theorem 2.3.2 that

$$N_q(\Lambda) \leq \left| \Lambda \setminus \bigcup_{i=1}^{m} (q\lambda_i + \Lambda) \right| + 1 \leq |\Lambda \setminus (q\lambda_1 + \Lambda)| + 1 = q\lambda_1 + 1,$$

where the equality is obtained by proposition 2.3.4. □

Remark. Notice that this version of the Lewittes bound applies the smallest non-zero element λ_1 in the Weierstraß semigroup, whereas the original bound just applied some pole number n. Thus, by possessing information about the structure of Λ, one might obtain a stronger bound from corollary 2.3.5 than from theorem 2.2.11. With λ_1 we have the strongest version of the bound, but even if we know nothing about Λ, we still know that $\lambda_1 \leq g + 1$ since Λ always has g gaps due to theorem 1.2.3. Thus, a worst-case version of the bound would use $\lambda_1 = g + 1$, for which we only need knowing the genus of the function field.

We now give an example, comparing the bounds presented in theorem 2.3.2 and corollary 2.3.5.

Example 2.3.6:
Consider the numerical semigroup $\Lambda = \langle 6, 10, 11 \rangle$ of genus $g = 13$. Let $L_q(\Lambda)$ denote the bound given in corollary 2.3.5 and $GM_q(\Lambda)$ denote the bound given in theorem 2.3.2. Then we obtain

q	2	3	4	5	7	8
$L_q(\Lambda)$	13	19	25	31	43	49
$GM_q(\Lambda)$	9	17	25	30	43	49

for the first few values of q. In fact, for $q \geq 7$, $L_q(\Lambda)$ and $GM_q(\Lambda)$ will always agree for this specific semigroup. Notice also that the bounds agree for $q = 4$ as well, but they disagree for $q = 5$. We will examine this in more detail later in the section. ◁

As with the Serre bound, we show that the Lewittes and the Geil-Matsumoto bounds are optimal in the sense that there exist function fields that meet each bound. For the Lewittes bound, it follows directly from corollary 2.3.5 for $\lambda_1 = q$ and alphabet size q^2. Thus, the corresponding Hermitian function field meets the bound given in equation (2.12). Furthermore, it turns out that the Hermitian function fields are maximal with respect to the Geil-Matsumoto bound in the sense that they possess the largest possible number of rational places for any function field with Weierstraß semigroup $\Lambda = \langle q, q + 1 \rangle$.

Proposition 2.3.7:
Let $\Lambda = \langle q, q+1 \rangle$ and let H denote the Hermitian function field over $\mathbb{F}_{q^2}$. Then

$$N(H) = N_{q^2}(\Lambda).$$

Proof. Recall that $N(H) = q^3 + 1$. We have $\lambda_1 = q$ and $\lambda_2 = q+1$. Applying (2.10) we thus need to show that

$$\left| \Lambda \setminus ((q^2 \cdot q + \Lambda) \cup (q^2 \cdot (q+1) + \Lambda)) \right| = q^3.$$

Note that since $q \in \Lambda$, we have $(q^3+q^2+\Lambda) \subseteq (q^3+\Lambda)$, meaning that $(q^3+q+\Lambda) \cup (q^3+\Lambda) = q^3 + \Lambda$. Now, by proposition 2.3.4, the result follows. □

We wish to examine how the Geil-Matsumoto bound on $N_q(\Lambda)$ can be interpreted as a bound determined by q and g alone. We begin by the following consequence of theorem 2.3.2.

Corollary 2.3.8:
Let $t \coloneqq \left| \{\lambda \in \Lambda : \lambda \in [\lambda_1 + 1, \lambda_1 + \lceil \frac{\lambda_1}{q} \rceil - 1]\} \right|$. Then $N_q(\Lambda)$ satisfies

$$N_q(\Lambda) \leq q\lambda_1 - t + 1.$$

Proof. Recall that $\Lambda = \langle \lambda_1, \ldots, \lambda_m \rangle$ with $0 < \lambda_1 < \cdots < \lambda_m$, thus there is no non-zero $\zeta \in \Lambda$ such that $\zeta < \lambda_1$. Since $\lceil \frac{\lambda_1}{q} \rceil - 1 < \frac{\lambda_1}{q}$, it holds for $\lambda \in [\lambda_1 + 1, \lambda_1 + \lceil \frac{\lambda_1}{q} \rceil - 1]$ that $q\lambda = q\lambda_1 + \zeta$ for $\zeta \in [q, \lambda_1)$. But since no such ζ exists, we have $q\lambda \neq q\lambda_1 + \zeta$ for any non-zero $\zeta \in \Lambda$. But then $q\lambda \in \bigcup_{i=1}^{m} (q\lambda_i + \Lambda) \setminus (q\lambda_1 + \Lambda)$ so we have the bound

$$\left| \bigcup_{i=1}^{m} (q\lambda_i + \Lambda) \setminus (q\lambda_1 + \Lambda) \right| \geq t.$$

This means that we remove at least t more elements in theorem 2.3.2 than in corollary 2.3.5, and the result follows. □

Proposition 2.3.9:
Let $F/\mathbb{F}_q$ be a function field. Then N satisfies

$$N \leq \left(q - \frac{1}{q} \right) (g+1) + 2.$$

Proof. We wish to determine a bound on t only by using λ_1 and g. We first have

$$\left| [\lambda_1 + 1, \lambda_1 + \left\lceil \frac{\lambda_1}{q} \right\rceil - 1] \right| = \left(\lambda_1 + \left\lceil \frac{\lambda_1}{q} \right\rceil - 1 \right) - (\lambda_1 + 1) + 1 = \left\lceil \frac{\lambda_1}{q} \right\rceil - 1.$$

Now, removing the $g - (\lambda_1 - 1)$ gaps greater than λ_1, we obtain

$$t \geq \left\lceil \frac{\lambda_1}{q} \right\rceil - 1 - (g - (\lambda_1 - 1)) \geq \frac{\lambda_1}{q} + \lambda_1 - g - 2.$$

Thus, by corollary 2.3.8, we have the bound

$$\begin{aligned} N &\leq \max_{2\leq\lambda_1\leq g+1}\left\{q\lambda_1 - \left(\frac{\lambda_1}{q} + \lambda_1 - g - 2\right) + 1\right\} \\ &= \left(q - \frac{1}{q}\right)(g+1) + 2, \end{aligned}$$

as desired, where clearly $\lambda_1 = g+1$ maximises the expression. Notice that we must uphold $2 \leq \lambda_1 \leq g+1$, since by theorem 1.2.3 there are exactly g gaps with 1 being one of them. Therefore, λ_1 must be greater than 1 but at most $g+1$. □

Example 2.3.10:
The bound from proposition 2.3.9 is derived from theorem 2.3.2 and must therefore be weaker than the Geil-Matsumoto bound. Consider the setup from example 2.3.3 where we assumed the existence of a function field $F/\mathbb{F}_2$ with a rational place admitting the Weierstraß semigroup $\Lambda = \langle 7, 10, 13, 18\rangle$ of genus $g = 15$. Recall that $N_2(\Lambda) \leq 9$. For comparison, we obtain by proposition 2.3.9 that $N \leq 26$. While not as strong as the Geil-Matsumoto estimate, it is still stronger than $N \leq 33$, which we obtained by the Serre bound. ◁

2.3.1 Closed form of bound for $\Lambda = \langle \lambda_1, \lambda_2\rangle$

Although functional in theory, the Geil-Matsumoto can be cumbersome to calculate in practice. In this section, we showcase a closed formula for the Geil-Matsumoto bound in equation (2.10) when Λ is generated by two elements λ_1, λ_2. Thus, for this section, assume that $\Lambda = \langle \lambda_1, \lambda_2\rangle$ where $\lambda_1 < \lambda_2$. Notice that this implies that λ_1 and λ_2 are coprime, since otherwise $|\mathbb{N}_0 \setminus \Lambda| = \infty$, contradicting the definition of a numerical semigroup. Although this may sound restrictive when considering specific function fields, it is worth noting that several widely used families of function fields possess rational places with Weierstraß semigroups that are generated by only two integers, most notably Hermitian function fields. Several of such function fields will be treated in the next chapter. This section is based on [Bras-Amorós et al., 2014].

We begin the section with a lemma.

Lemma 2.3.11:
Let ν be the inverse of λ_2 modulo λ_1. Then the following hold:

i. For each $\lambda \in \Lambda$ there exist unique $m, n \geq 0$ with $n \leq \lambda_1 - 1$ such that $\lambda = m\lambda_1 + n\lambda_2$.
ii. $\lambda \in \Lambda$ if and only if $\lambda_2(\lambda\nu \mod \lambda_1) \leq \lambda$.

Proof. *i.* We begin by showing existence. Thus, assume that $\lambda \in \Lambda$. By definition of Λ we can then write $\lambda = \alpha\lambda_1 + \beta\lambda_2$ for some $\alpha, \beta \in \mathbb{N}_0$. We can write $\beta = q\lambda_1 + r$ where $q \in \mathbb{Z}$ and $r = (\beta \mod \lambda_1)$. Then clearly we have $\frac{\beta}{\lambda_1} = q + \frac{r}{\lambda_1}$, implying that $\lfloor \frac{\beta}{\lambda_1} \rfloor = q$. Thus, we

can use $\lfloor \frac{\beta}{\lambda_1} \rfloor \lambda_1 + (\beta \mod \lambda_1) = q\lambda_1 + r = \beta$. We now let $m = \alpha + \lambda_2 \lfloor \frac{\beta}{\lambda_1} \rfloor$ and $n = (\beta \mod \lambda_1)$. Then we obtain

$$\begin{aligned}
\lambda &= \alpha\lambda_1 + \beta\lambda_2 \\
&= \alpha\lambda_1 + \left(\left\lfloor \frac{\beta}{\lambda_1} \right\rfloor \lambda_1 + (\beta \mod \lambda_1) \right) \lambda_2 \\
&= \left(\alpha + \lambda_2 \left\lfloor \frac{\beta}{\lambda_1} \right\rfloor \right) \lambda_1 + (\beta \mod \lambda_1)\lambda_2 \\
&= m\lambda_1 + n\lambda_2,
\end{aligned}$$

where we see that $m, n \geq 0$ and $n \leq \lambda_1 - 1$.

To show uniqueness, assume that $m\lambda_1 + n\lambda_2 = \lambda = \hat{m}\lambda_1 + \hat{n}\lambda_2$ where $m, n, \hat{m}, \hat{n} \geq 0$ and $n, \hat{n} \leq \lambda_1 - 1$. This implies that $(m - \hat{m})\lambda_1 = (\hat{n} - n)\lambda_2$, and since λ_1 and λ_2 are coprime we have $\lambda_1 | (\hat{n} - n)$ (see for example [Lauritzen, 2011; Corollary 1.5.10]). But this must mean that $\hat{n} = n$, and thus also $\hat{m} = m$.

ii. We begin by assuming that $\lambda \in \Lambda$. Then by point *i.* of this lemma we have $\lambda = m\lambda_1 + n\lambda_2$ for unique $m, n \geq 0$ with $n \leq \lambda_1 - 1$. We have

$$(\lambda\nu \mod \lambda_1) = \big((m\lambda_1 + n\lambda_2)\nu \mod \lambda_1\big) = (n\lambda_2\nu \mod \lambda_1) = n,$$

since $(\lambda_2\nu \mod \lambda_1) = 1$ by assumption. Thus, $\lambda_2(\lambda\nu \mod \lambda_1) = \lambda_2 n \leq \lambda$.

For the converse, consider some $\zeta \in \mathbb{N}_0$ and define $\beta = (\zeta\nu \mod \lambda_1)$. Then we have

$$\big((\zeta - \beta\lambda_2) \mod \lambda_1\big) = \big(((\zeta \mod \lambda_1) - (\beta\lambda_2 \mod \lambda_1)) \mod \lambda_1\big) = 0,$$

thus $\zeta - \beta\lambda_2$ is a multiple of λ_1. Moreover, if $\beta\lambda_2 \leq \zeta$, then $\zeta - \beta\lambda_2$ is a positive multiple of λ_1. In other words, there exists a positive integer α such that $\zeta - \beta\lambda_2 = \alpha\lambda_1$. Simply rearranging this, we obtain the conical combination $\zeta = \alpha\lambda_1 + \beta\lambda_2$, hence $\zeta \in \Lambda$. □

We now present a closed formula for computing the Geil-Matsumoto bound, when Λ is generated by only two integers.

Theorem 2.3.12:
For $\Lambda = \langle \lambda_1, \lambda_2 \rangle$ we have

$$\begin{aligned}
GM_q(\Lambda) &= 1 + \sum_{n=0}^{\lambda_1 - 1} \min \left\{ q, \left\lceil \frac{q-n}{\lambda_1} \right\rceil \lambda_2 \right\} \qquad (2.13) \\
&= \begin{cases} 1 + q\lambda_1, & q \leq \lfloor \frac{q}{\lambda_1} \rfloor \lambda_2 \\ 1 + (q \mod \lambda_1)q + (\lambda_1 - (q \mod \lambda_1))\lfloor \frac{q}{\lambda_1} \rfloor \lambda_2, & \lfloor \frac{q}{\lambda_1} \rfloor \lambda_2 < q < \lceil \frac{q}{\lambda_1} \rceil \lambda_2. \end{cases}
\end{aligned}$$

Proof. Recall the set from equation (2.10), that is

$$\Lambda \setminus \big((q\lambda_1 + \Lambda) \cup (q\lambda_2 + \Lambda)\big) =: \mathcal{U}$$

for $\Lambda = \langle \lambda_1, \lambda_2 \rangle$. If $\zeta \in \mathcal{U}$ then $\zeta \notin q\lambda_i + \Lambda$ for $i = 1, 2$. Equivalently, we have $\zeta \neq q\lambda_i + \lambda$ for $i = 1, 2$ and $\lambda \in \Lambda$. This then gives us $\zeta - q\lambda_i \notin \Lambda$ for $i = 1, 2$. We can therefore rewrite the Geil-Matsumoto bound as $1 + |\{\lambda \in \Lambda : \lambda - q\lambda_i \notin \Lambda, i = 1, 2\}|$. We begin by examining what implications the conditions $\lambda - q\lambda_i \notin \Lambda$ might have for $\lambda \in \Lambda$. Let m and n be the unique integers such that $\lambda = m\lambda_1 + n\lambda_2$ with $m, n \geq 0$ and $n \leq \lambda_1 - 1$. We have

$$\lambda - q\lambda_1 \notin \Lambda \iff q > m, \tag{2.14}$$

as well as

$$\lambda - q\lambda_2 \notin \Lambda \iff \lambda_2 \left\lceil \frac{q-n}{\lambda_1} \right\rceil > m, \tag{2.15}$$

The intermediate steps are omitted in equations (2.14) and (2.15), but can be found in appendix A.1. Thus, the number of elements $\lambda \in \Lambda$ that satisfy both of these conditions must equal

$$\sum_{n=0}^{\lambda_1 - 1} \min \left\{ q, \left\lceil \frac{q-n}{\lambda_1} \right\rceil \lambda_2 \right\} =: S. \tag{2.16}$$

We now examine what (2.16) reduces into depending on the value of q. First, say we want every term in the sum to be equal to q. Then we must have $q \leq \lceil \frac{q-(\lambda_1-1)}{\lambda_1} \rceil \lambda_2$, as this guarantees that q be the smallest element in every term. In this case, $S = \lambda_1 q$. On the other hand, we have the upper bound

$$\left\lceil \frac{q-n}{\lambda_1} \right\rceil \lambda_2 \leq \left\lceil \frac{q}{\lambda_1} \right\rceil \lambda_2,$$

for $n = 0, 1, \ldots, \lambda_1 - 1$. Since no value of q can satisfy $q \geq \lceil \frac{q}{\lambda_1} \rceil \lambda_2$, we only need to consider the case where $\lceil \frac{q-\lambda_1+1}{\lambda_1} \rceil \lambda_2 < q < \lceil \frac{q}{\lambda_1} \rceil \lambda_2$. We exploit the fact that we can write $q = \lambda_1 s + r$, where $s = \lfloor \frac{q}{\lambda_1} \rfloor$ and $r = (q \mod \lambda_1)$. Then we obtain

$$\left\lceil \frac{q-n}{\lambda_1} \right\rceil = \left\lceil \frac{\lambda_1 s + r - n}{\lambda_1} \right\rceil = \left\lceil s + \frac{r-n}{\lambda_1} \right\rceil = \begin{cases} s+1, & n < r \\ s, & n \geq r. \end{cases}$$

From this observation, we may rewrite the sum as

$$S = \sum_{n=0}^{r-1} \min \left\{ q, (s+1)\lambda_2 \right\} + \sum_{n=r}^{\lambda_1 - 1} \min\{q, s\lambda_2\}. \tag{2.17}$$

We now take a closer look at s. Observe the rational numbers $\frac{q}{\lambda_1}$ and $\frac{q-\lambda_1+1}{\lambda_1}$. Notice that

$$\frac{q}{\lambda_1} - \frac{q-\lambda_1+1}{\lambda_1} = \frac{\lambda_1 - 1}{\lambda_1} < 1.$$

Thus, there is only a single integer between $\frac{q}{\lambda_1}$ and $\frac{q-\lambda_1+1}{\lambda_1}$, so

$$\left\lceil \frac{q-\lambda_1+1}{\lambda_1} \right\rceil = \left\lfloor \frac{q}{\lambda_1} \right\rfloor = s.$$

This further implies that $s\lambda_2 < q$, since we assumed in this case that $q > \lceil \frac{q-\lambda_1+1}{\lambda_1} \rceil \lambda_2$. Additionally, we have $s+1 = \lfloor \frac{q}{\lambda_1} \rfloor + 1 \geq \lceil \frac{q}{\lambda_1} \rceil$, which implies that $(s+1)\lambda_2 > q$. Applying this knowledge to equation (2.17), we get

$$S = rq + (\lambda_1 - r)s\lambda_2 = (q \mod \lambda_1)q + (\lambda_1 - (q \mod \lambda_1)) \left\lfloor \frac{q}{\lambda_1} \right\rfloor \lambda_2. \tag{2.18}$$

Finally, using $\lfloor \frac{q}{\lambda_1} \rfloor = \lceil \frac{q-\lambda_1+1}{\lambda_1} \rceil$ in the bounds for q, we obtain the desired result. □

2.3.2 Comparison of Lewittes' and Geil-Matsumoto bounds

Recall example 2.3.6 where we saw that the Lewittes and Geil-Matsumoto bounds agreed from some values of q. These next results, most of which can be found in [Bras-Amorós et al., 2014], give a theoretical guarantee for when this behaviour occurs. We once again apply the notions $L_q(\Lambda)$ and $GM_q(\Lambda)$.

Proposition 2.3.13:
Let Λ be fixed. Then $L_q(\Lambda) = GM_q(\Lambda)$ if and only if $q(\lambda_i - \lambda_1) \in \Lambda$ for $i = 2, 3, \ldots, m$.

Proof. We first note that by corollary 2.3.5, the statement $L_q(\Lambda) = GM_q(\Lambda)$ is equivalent to

$$\left| \Lambda \setminus \bigcup_{i=1}^{m} (q\lambda_i + \Lambda) \right| = |\Lambda \setminus (q\lambda_1 + \Lambda)|.$$

Then the result follows from

$$\begin{aligned} \left| \Lambda \setminus \bigcup_{i=1}^{m} (q\lambda_i + \Lambda) \right| = |\Lambda \setminus (q\lambda_1 + \Lambda)| &\iff q\lambda_i + \Lambda \subseteq q\lambda_1 + \Lambda \\ &\iff q\lambda_i \in q\lambda_1 + \Lambda \\ &\iff q(\lambda_i - \lambda_1) \in \Lambda, \end{aligned}$$

where all statements hold for $i = 2, 3, \ldots, m$. □

Example 2.3.14:
Consider once again $\Lambda = \langle 6, 10, 11 \rangle$ from example 2.3.6. Computing $q(\lambda_i - \lambda_1)$ for $i = 2, 3$, we obtain

q	4	5	7	8
$q(\lambda_2 - \lambda_1)$	16	20	28	32
$q(\lambda_3 - \lambda_1)$	20	25	35	40

for a few select values of q. Since Λ is given by

$$\Lambda = \{0, 6, 10, 11, 12, 16, 17, 18, 20, 21, 22, 23, 24\} \cup \{i \in \mathbb{N}_0 | i \geq 26\},$$

we see that $L_q(\Lambda) = GM_q(\Lambda)$ for $q = 4, 7, 8$, whereas $25 \notin \Lambda$, hence the bounds do not agree for $q = 5$. In fact, 25 is the Frobenius number of the set $\{6, 10, 11\}$, so if $q(\lambda_i - \lambda_1) > 25$ then it is guaranteed to be in Λ. $\lhd$

The observation in example 2.3.14 leads to another condition for determining when $L_q(\Lambda) = GM_q(\Lambda)$.

Corollary 2.3.15:
Let Λ be fixed and let $\mathcal{F}$ denote the Frobenius number of the generating set of Λ. Then $L_q(\Lambda) = GM_q(\Lambda)$ if $q(\lambda_i - \lambda_1) > \mathcal{F}$ for $i = 2, 3, \ldots, m$.

A simpler, albeit weaker, condition is just for q to be larger than $\mathcal{F}$, since $\lambda_i - \lambda_1 \geq 1$ for $i = 2, 3, \ldots, m$. In fact, if $q \in \Lambda$ then necessarily $q(\lambda_i - \lambda_1) \in \Lambda$ for $i = 2, 3, \ldots, m$ as well. Thus, $q \in \Lambda$ is another sufficient condition for the two bounds being equal. However, corollary 2.3.15 is not that strong a condition. Using this condition alone on the semigroup from example 2.3.14, we only guarantee $L_q(\Lambda) = GM_q(\Lambda)$ for $q > 5$, but as we have seen they agree for $q = 4$ as well. Since $4 \notin \Lambda$, we cannot use the condition $q \in \Lambda$ either. Secondly, determining the Frobenius number of any given set of generators is known to be hard. The condition presented in proposition 2.3.13 is a good condition, however it requires us to check all the generators of Λ. In the following, we describe a condition in the hope that it will include cases such as $q = 4$ in example 2.3.14 while also requiring fewer comparisons. For the next lemma, we use the notation $c\langle \alpha, \beta \rangle = \{c\gamma : \gamma \in \langle \alpha, \beta \rangle\}$.

Lemma 2.3.16:
Let i be fixed such that $2 \leq i \leq m$ and let $d \coloneqq \gcd(\lambda_1, \lambda_i)$. Then $q(\lambda_i - \lambda_1) \in d\langle \frac{\lambda_1}{d}, \frac{\lambda_i}{d} \rangle$ if and only if $qd \leq \lfloor \frac{qd}{\lambda_1} \rfloor \lambda_i$.

Proof. We first assume that $q(\lambda_i - \lambda_1) \in d\langle \frac{\lambda_1}{d}, \frac{\lambda_i}{d} \rangle$ and rewrite it as $q(\frac{\lambda_i}{d} - \frac{\lambda_1}{d}) \in \langle \frac{\lambda_1}{d}, \frac{\lambda_i}{d} \rangle$. Let ν denote the inverse of $\frac{\lambda_i}{d}$ modulo $\frac{\lambda_1}{d}$. Then lemma 2.3.11*ii.* tells us that

$$\begin{aligned} q\left(\frac{\lambda_i}{d} - \frac{\lambda_1}{d}\right) \in \left\langle \frac{\lambda_1}{d}, \frac{\lambda_i}{d} \right\rangle &\iff \frac{\lambda_i}{d}\left(q\left(\frac{\lambda_i}{d} - \frac{\lambda_1}{d}\right)\nu \mod \frac{\lambda_1}{d}\right) \leq q\left(\frac{\lambda_i}{d} - \frac{\lambda_1}{d}\right) \\ &\iff \frac{\lambda_i}{d}\left(q \mod \frac{\lambda_1}{d}\right) \leq q\left(\frac{\lambda_i}{d} - \frac{\lambda_1}{d}\right) \\ &\iff qd \leq \left\lfloor \frac{qd}{\lambda_1} \right\rfloor \lambda_i. \end{aligned}$$

Several details leading to the last equivalence are omitted here, but can be found in appendix A.2. $\square$

We elucidate the usefulness of lemma 2.3.16. We are interested in a, possibly stronger, condition that implies $q(\lambda_i - \lambda_1) \in \Lambda$ for $i = 2, 3, \ldots, m$. We fix i such that $2 \leq i \leq m$ and instead focus on when $q(\lambda_i - \lambda_1) \in \langle \lambda_1, \lambda_i \rangle$ as this naturally implies that $q(\lambda_i - \lambda_1) \in \Lambda$. Let

$d \coloneqq \gcd(\lambda_1, \lambda_i)$. Then clearly $\langle \lambda_1, \lambda_i \rangle = d\langle \frac{\lambda_1}{d}, \frac{\lambda_i}{d} \rangle$. By these arguments and lemma 2.3.16 we obtain

$$q(\lambda_i - \lambda_1) \in \Lambda \iff qd \leq \lambda_i \left\lfloor \frac{qd}{\lambda_1} \right\rfloor.$$

Further, assume that $q \leq \lfloor \frac{q}{\lambda_1} \rfloor \lambda_i$. Then we have directly that

$$qd \leq \left\lfloor \frac{q}{\lambda_1} \right\rfloor \lambda_i d \leq \left\lfloor \frac{qd}{\lambda_1} \right\rfloor \lambda_i,$$

thus $q \leq \lfloor \frac{q}{\lambda_1} \rfloor \lambda_i$ is a sufficient condition for $L_q(\Lambda) = GM_q(\Lambda)$. Moreover, since $\lambda_1 < \lambda_2 < \cdots < \lambda_m$ by assumption, it suffices to check that $q \leq \lfloor \frac{q}{\lambda_1} \rfloor \lambda_2$. We summarise these considerations in the following result.

Proposition 2.3.17:
Let Λ be fixed. If $q \leq \lfloor \frac{q}{\lambda_1} \rfloor \lambda_2$, then $L_q(\Lambda) = GM_q(\Lambda)$.

It is worth mentioning that the converse is not generally true, however in the case $\Lambda = \langle \lambda_1, \lambda_2 \rangle$ it holds in both directions, as was also shown in theorem 2.3.12. In general, one can easily find counterexamples where $L_q(\Lambda) = GM_q(\Lambda)$ but $q > \lfloor \frac{q}{\lambda_1} \rfloor \lambda_2$. For instance, take a look at example 2.3.14. Applying proposition 2.3.17 for $q = 4$, we gather that $\lfloor \frac{4}{6} \rfloor \cdot 10 = 0 < 4$, however we have already established that $L_4(\Lambda) = GM_4(\Lambda)$ for $\Lambda = \langle 6, 10, 11 \rangle$. For more counterexamples, see for instance [Bras-Amorós et al., 2014; Remark 4.4].

Example 2.3.18:
Consider the numerical semigroup $\Lambda = \langle 11, 13 \rangle$ of genus $g = 60$. For a script that computes the numerical semigroup generated by two coprime integers, see appendix B.2. We define $q_1 \coloneqq 16$ and $q_2 \coloneqq 64$. Notice that $\lfloor \frac{16}{11} \rfloor \cdot 13 = 13$, thus $q_1 > \lfloor \frac{q_1}{\lambda_1} \rfloor \lambda_2$. Similarly, we see that $\lfloor \frac{64}{11} \rfloor \cdot 13 = 65$, so $q_2 < \lfloor \frac{q_2}{\lambda_1} \rfloor \lambda_2$. Comparing the original Geil-Matsumoto bound, the closed form from theorem 2.3.12 and the Lewittes bound from corollary 2.3.5, we obtain $GM_{q_1}(\Lambda) = 159$ from both versions of the Geil-Matsumoto bound and $L_{q_1}(\Lambda) = 177$ from Lewittes' bound. This is in accordance with proposition 2.3.17. On the other hand, we obtain $N \leq 705$ from all three calculations for q_2, once again as expected from proposition 2.3.17.$\lhd$

2.3.3 Upper bound for when $L_q(\Lambda) \neq GM_q(\Lambda)$

We conclude the section by giving an alternative assessment to proposition 2.3.17. The formula given in theorem 2.3.12 yields alternating outputs due to the conditions on q, hence it is not always clear for which value of q it holds that $L_q(\Lambda) = GM_q(\Lambda)$. This motivates the following result, which still holds in general due to it depending on proposition 2.3.17. Given a fixed numerical semigroup Λ, we are interested in knowing if the Lewittes and Geil-Matsumoto bounds are equal for all $q > M$ for some $M \in \mathbb{N}$. We know from proposition 2.3.17 that the bounds are equal if

$$q \leq \left\lfloor \frac{q}{\lambda_1} \right\rfloor \lambda_2. \tag{2.19}$$

We make the following bound, from which point the two bounds always agree.

Proposition 2.3.19:
Let Λ be fixed and let $\gamma = \lceil \frac{\lambda_1}{\lambda_2 - \lambda_1} \rceil$. Then $L_q(\Lambda) = GM_q(\Lambda)$ for all $q \geq \gamma\lambda_1$.

Proof. We first examine the growth of the right hand side of the inequality in (2.19) with respect to the left hand side. If $0 \leq q < \lambda_1$, then $\lfloor \frac{q}{\lambda_1} \rfloor \lambda_2 = 0$, so for q in this interval, we always have $q \geq \lfloor \frac{q}{\lambda_1} \rfloor \lambda_2$. Further, if $\lambda_1 \leq q < 2\lambda_1$, then $\lfloor \frac{q}{\lambda_1} \rfloor \lambda_2 = \lambda_2$, so $q \leq \lfloor \frac{q}{\lambda_1} \rfloor \lambda_2$ if $2\lambda_1 < \lambda_2$. In general, we have for $\gamma\lambda_1 \leq q < (\gamma+1)\lambda_1$ that $\lfloor \frac{q}{\lambda_1} \rfloor \lambda_2 = \gamma\lambda_2$. Now, if $\gamma \in \mathbb{Z}$ and $(\gamma+1)\lambda_1 \leq \gamma\lambda_2$, then (2.19) is satisfied, thus the result holds by proposition 2.3.17. We now wish to determine the smallest such γ. Isolating γ in $(\gamma+1)\lambda_1 \leq \gamma\lambda_2$, we obtain $\gamma \geq \frac{\lambda_1}{\lambda_2 - \lambda_1}$, so to guarantee both that the inequality remains true and that $\gamma \in \mathbb{Z}$, we set $\gamma = \lceil \frac{\lambda_1}{\lambda_2 - \lambda_1} \rceil$. Now, by the assumptions that $(\gamma+1)\lambda_1 \leq \gamma\lambda_2$ and $\lambda_1 < \lambda_2$, the inequality in (2.19) holds for all $q \geq \gamma\lambda_1$ so by proposition 2.3.17 we obtain the desired result. □

We note that proposition 2.3.19 does not generally guarantee that $L_q(\Lambda) \neq GM_q(\Lambda)$ for any q, however for $\Lambda = \langle \lambda_1, \lambda_2 \rangle$ we know that at least one value of q less than $\gamma\lambda_1$ results in the bounds disagreeing. In the possible interest of having a function field with the property that the Geil-Matsumoto bound for said function field is stronger than the Lewittes bound, it is shown in [Beelen, 2007] that given a numerical semigroup $\Lambda = \langle \lambda_1, \lambda_2 \rangle$, one can obtain the equation of a function field that has a place with Weierstraß semigroup equal to Λ. For this function field, at least one value of $q < \gamma\lambda_1$ provides $GM_q(\Lambda) < L_q(\Lambda)$.

We exemplify the behaviour of the inequality in (2.19) leading up to the bound given in proposition 2.3.19. Note that for this purpose, we let q be any natural number. It is important to note that because of this, the bounds yield values that, for some choices of q, are meaningless in the sense of bounding the number of rational places, since it is well known that all finite fields are of order p^n with p prime. Nonetheless, we allow $q \in \mathbb{N}_0$ in order to easier visualise the behaviour of (2.19).

Example 2.3.20:
Consider once again the numerical semigroup $\Lambda = \langle 11, 13 \rangle$. For $0 < q < 11$, the bounds yield

q	1	2	3	4	5	6	7	8	9	10
$L_q(\Lambda)$	12	23	34	45	56	67	78	89	100	111
$GM_q(\Lambda)$	2	5	10	17	26	37	50	65	82	101

Technically, the bounds agree for $q = 0$, for which they both output 1. For $11 \leq q < 22$, the bounds agree when $q = 11, 12, 13$. For the k'th interval, the bounds only agree when $q \leq \min\{(k+1)\lambda_1, k\lambda_2\}$. The difference between $L_q(\Lambda)$ and $GM_q(\Lambda)$ for $1 \leq q \leq 70$ can be seen in figure 2.2.

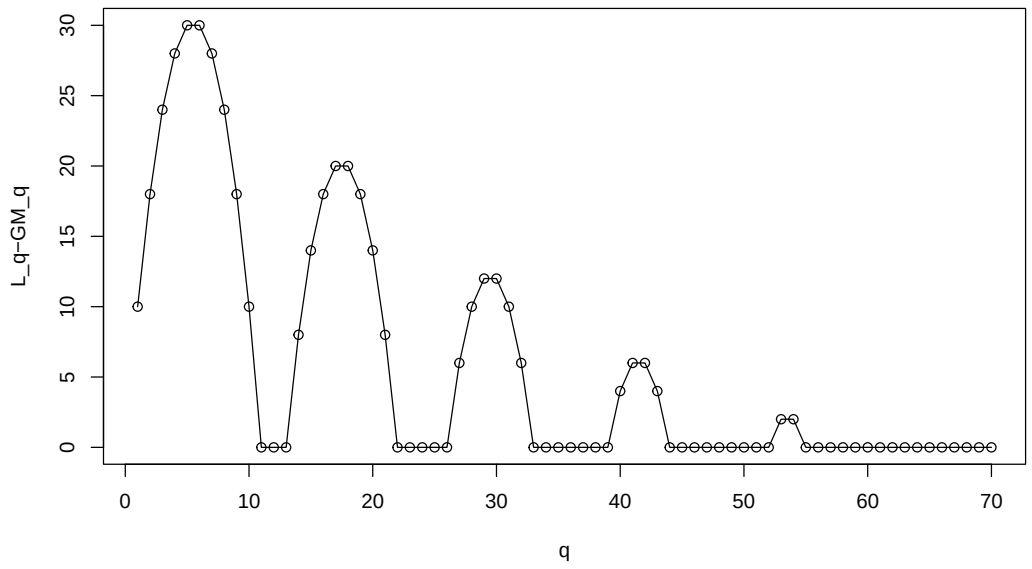

Figure 2.2: The difference between $L_q(\Lambda)$ and $GM_q(\Lambda)$ for $1 \leq q \leq 70$.

Let $\gamma = \lceil \frac{11}{13-11} \rceil = 6$. Thus, for $q \geq \gamma\lambda_1 = 66$, the bounds always agree. For the γ'th interval, we have $66 \leq q < 77$, in which case $\lfloor \frac{q}{\lambda_1} \rfloor \lambda_2 = 78$. Since adding λ_1 to the left hand side leads to an increase of λ_2 on the right hand side, and $\lambda_2 > \lambda_1$, we no longer risk any values of q to imply that $L_q(\Lambda) \neq GM_q(\Lambda)$.

Notice that for the case of $\Lambda = \langle 11, 13 \rangle$, the bounds already agree from $q \geq \lfloor \frac{\lambda_1}{\lambda_2 - \lambda_1} \rfloor \lambda_1 = 55$, that is, from $(\gamma - 1)\lambda_1$. This does not always hold, even for numerical semigroups generated by two integers. If $\Lambda = \langle 14, 17 \rangle$, then $\lfloor \frac{\lambda_1}{\lambda_2 - \lambda_1} \rfloor \lambda_1 = 56$. However, $L_{69}(\Lambda) = 967$ and $GM_{69}(\Lambda) = 966$. $\lhd$

Evaluating the definition of γ in proposition 2.3.19, we conclude that in order for the Geil-Matsumoto bound to be as strong as possible in comparison to the Lewittes bound, we want λ_1 to be large and $\lambda_2 - \lambda_1$ to be small. This leaves the largest possible space for q to yield different values for $L_q(\Lambda)$ and $GM_q(\Lambda)$. For example, a visualisation of the difference between the two bounds for $\Lambda = \langle 29, 31 \rangle$ can be seen in figure 2.3.

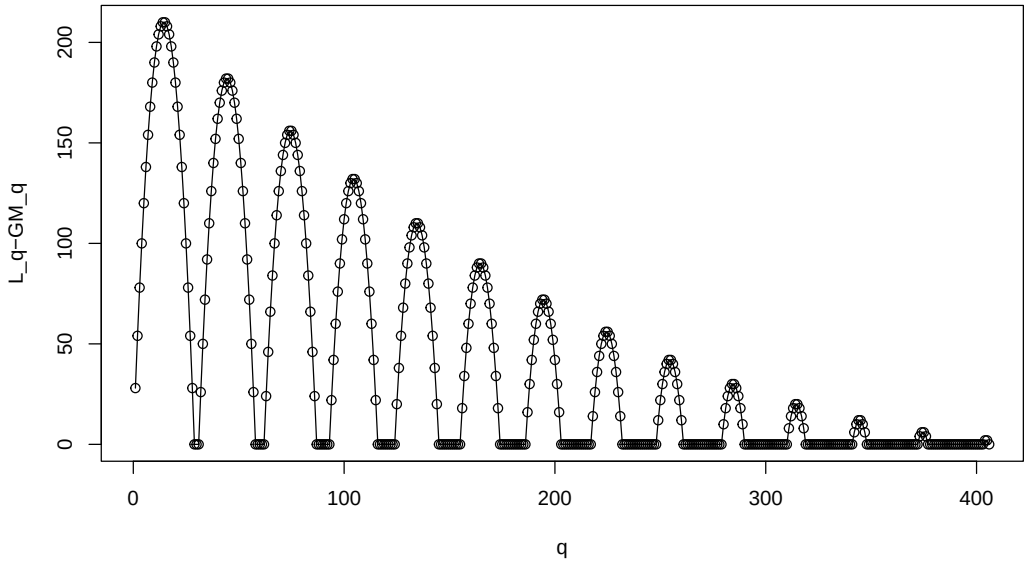

Figure 2.3: The difference between $L_q(\Lambda)$ and $GM_q(\Lambda)$ for $\Lambda = \langle 29, 31 \rangle$.

The formula in theorem 2.3.12 also suggests that for the strongest improvement over the Lewittes bound, one requires q relatively small as we will examine in the following. This is also exemplified in figure 2.4.

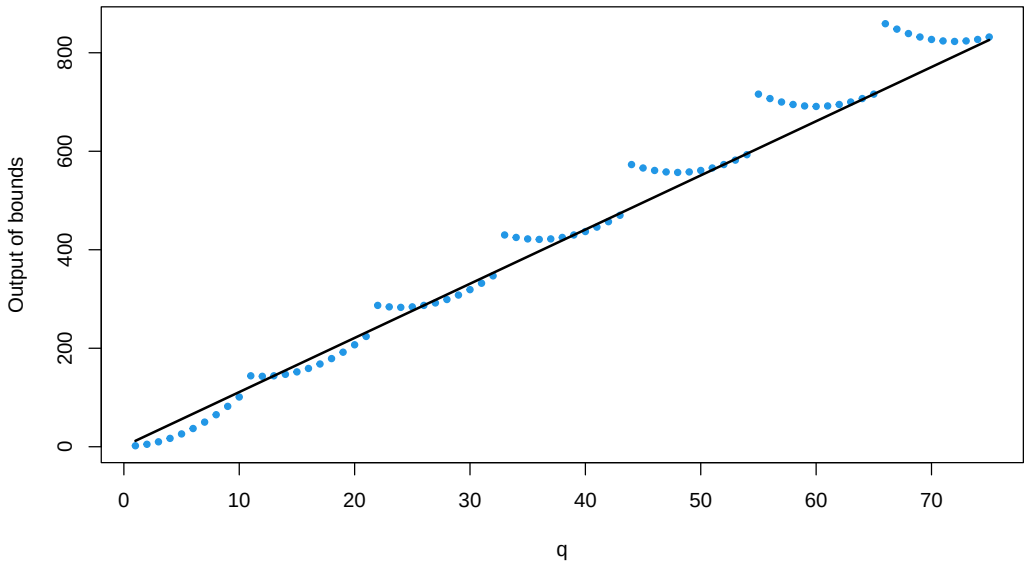

Figure 2.4: $L_q(\Lambda)$ and $\varpi_q(\Lambda)$ for $\Lambda = \langle 11, 13 \rangle$. The black line represents $L_q(\Lambda)$; the blue circles represent $\varpi_q(\Lambda)$.

Here, we have plotted the outputs of each of the two expressions in the formula from theorem 2.3.12. For this examination, we once again apply $\Lambda = \langle 11, 13\rangle$ for the sake of visual clarity. For the remainder of this discussion, we refer to the first expression simply as the Lewittes bound, and to the second expression as $\varpi_q(\Lambda)$ defined by

$$\varpi_q(\Lambda) \coloneqq 1 + (q \mod \lambda_1)q + (\lambda_1 - (q \mod \lambda_1)) \left\lfloor \frac{q}{\lambda_1} \right\rfloor \lambda_2.$$

Notice that due to the $(q \mod \lambda_1)q$ in $\varpi_q(\Lambda)$, we obtain arcs consisting of λ_1 points, each arc increasing in magnitude. The second term in $\varpi_q(\Lambda)$ transforms the arcs towards a descending line as q increases. We see that this expression yields smaller outputs than the Lewittes bound at first; then it gradually increases, thus making the difference smaller in each arc, as can be seen in figure 2.2. Reaching the point $q = (\gamma - 1)\lambda_1 - 1 = 54$, the last blue circle can be seen under the black line. Specifically, for $\Lambda = \langle 11, 13\rangle$, we have $L_{54}(\Lambda) = 595$ and $\varpi_{54}(\Lambda) = 593$. At $q = 55$ a new arc begins, and at its last point, that is, at $q = \gamma\lambda_1 - 1 = 65$, we obtain $L_{65}(\Lambda) = \varpi_{65}(\Lambda) = 716$. From this point, every arc will be strictly above the black line, and from proposition 2.3.19 we know that the two bounds agree for all q from this point.

One caveat that might arise from this approach at constructing function fields, for which the Geil-Matsumoto bound is particularly strong, is that the function field consequently will have a large genus.

Example 2.3.21:
Consider the numerical semigroup $\Lambda = \langle 101, 103\rangle$. Suppose that $F/\mathbb{F}_q$ is a function field with a rational place P having Λ as Weierstraß semigroup. Let $q = 49$. Then the Lewittes bound gives us $L_{49}(\Lambda) = 4950$. On the contrary, the Geil-Matsumoto yields a much smaller $GM_{49}(\Lambda) = 2402$, less than half the estimate given by Lewittes' bound. A function field such as this, however, is of genus $g = 5100$. As previously mentioned, in order to obtain good codes, we need g to be small compared to n. In this case, the genus is more than twice as large as the number of rational places, by the estimate given by $GM_q(\Lambda)$. ◁

2.4 The Beelen-Ruano Bound

Having examined a bound on $N(F)$ that applies knowledge of the Weierstraß semigroup of a single rational place of the function field, one question begs to be asked: can one obtain a stronger bound by assuming additional knowledge in a more generalised form? One such bound has been proposed in [Beelen et al., 2013], which applies a similar strategy as was used in proving the Geil-Matsumoto bound. Instead of restricting ourselves to utilising a single rational place P and its Weierstraß semigroup $H(P)$, we define a sort of generalised Weierstraß semigroup for a divisor based on a number of rational places.

In this section, we introduce this generalised structure and showcase the generalised bound it provides, which we shall refer to as the Beelen-Ruano bound. We discuss how to com-

pute the bound in practice and give arguments that supports the fact that the Geil-Matsumoto bound is a special case of this new bound.

Consider a function field $F/\mathbb{F}_q$ and let $P_1, \ldots, P_n \in \mathbb{P}_F$ be rational places. Denote by Ψ the set consisting of the $N(F) - n$ remaining rational places of $F/\mathbb{F}_q$. We also introduce some notions for integer n-tuples. As such, we consider $\iota = (\iota_1, \ldots, \iota_n) \in \mathbb{Z}^n$. We associate ι with Riemann-Roch spaces and degrees by considering the divisor $D_\iota = \sum_{j=1}^n \iota_j P_j$. Then we define $\deg \iota \coloneqq \deg D_\iota$ and $\mathscr{L}(\iota) \coloneqq \mathscr{L}(D_\iota)$. We will by $e_j \in \mathbb{Z}^n$ denote the usual canonical unit vector with 1 in the j'th entry and 0 elsewhere. Then we have for instance that $D_{\lambda e_j} = \lambda P_j$, thus $\mathscr{L}(\lambda e_j) = \mathscr{L}(\lambda P_j)$. This last relation is important in the following definition.

Definition 2.4.1:
Let $\iota \in \mathbb{Z}^n$. Then we define

$$H_\iota(P_j) \coloneqq \left\{ -v_{P_j}(z) : z \in \bigcup_{k \in \mathbb{Z}} \mathscr{L}(\iota + ke_j) \setminus \{0\} \right\}.$$

Notice that for $\iota = 0$ we have

$$H_0(P_j) = \left\{ -v_{P_j}(z) : z \in \bigcup_{k \in \mathbb{Z}} \mathscr{L}(kP_j) \setminus \{0\} \right\} = H(P_j).$$

Thus, in the trivial case, $H_0(P_j)$ reduces to the usual Weierstraß semigroup of P_j. Likewise, for $n = 1$, we have that $\iota \in \mathbb{Z}$, so

$$H_\iota(P) = \left\{ -v_P(z) : z \in \bigcup_{k \in \mathbb{Z}} \mathscr{L}((\iota + k)P) \setminus \{0\} \right\} = H(P).$$

Furthermore, consider the cases where $k < -\deg \iota$. Then we have

$$\deg(\iota + ke_j) = \deg \iota + k \deg e_j = \deg \iota + k < 0,$$

thus, $\mathscr{L}(\iota + ke_j) = \{0\}$. We can therefore omit these cases an instead write

$$H_\iota(P_j) = \left\{ -v_{P_j}(z) : z \in \bigcup_{k \geq -\deg \iota} \mathscr{L}(\iota + ke_j) \setminus \{0\} \right\}.$$

The idea behind the definition of $H_\iota(P_j)$ is to describe some quasi-generalised Weierstraß semigroup. In fact, the notion in definition 2.4.1 is related to the generalised Weierstraß semigroups studied by Beelen and Tutaş in [Beelen et al., 2006]. Instead of considering functions with pole divisor $(z)_\infty = \lambda P$, we accept more general pole divisors of the form $(z)_\infty = \lambda_1 P_1 + \cdots + \lambda_n P_n$. The goal is for these sets to provide a foundation for a generalisation of the Geil-Matsumoto bound. As such, we employ a similar strategy to construct this new bound. Recall that the proof for theorem 2.3.2 revolved around determining when the dimensions of certain Riemann-Roch spaces increased. We generalise this notion a bit in the following definition.

Definition 2.4.2:
*Let $\iota \in \mathbb{Z}^n$ and let $1 \leq j \leq n$ be an integer. If $\mathscr{L}(\iota) = \mathscr{L}(\iota + e_j)$ or if there exists a non-zero pole number $\lambda \in H(P_j)$ and a $\mu \in H_\iota(P_j)$ such that $\mu + q\lambda = \iota_j + 1$, we say that the pair $(\iota, \iota + e_j)$ is **negligible**. Additionally, we define the function*

$$\delta(\iota, \iota + e_j) := \begin{cases} 0, & \text{if } (\iota, \iota + e_j) \text{ is negligible}, \\ 1, & \text{otherwise}. \end{cases}$$

Remark. Note that definition 2.4.2 provides a generalised notion of the expression we used for the value t in the proof of theorem 2.3.2.

Lemma 2.4.3:
Let $(\iota, \iota + e_j)$ be negligible such that $\mathscr{L}(\iota) \subsetneq \mathscr{L}(\iota + e_j)$, and let $\lambda \in H(P_j)$ and $\mu \in H_\iota(P_j)$ such that $\mu + q\lambda = \iota_j + 1$. Then there exist functions $f \in \mathscr{L}(\lambda e_j)$ and $g \in \mathscr{L}(\iota)$ such that $f^q g \in \mathscr{L}(\iota + e_j) \setminus \mathscr{L}(\iota)$.

Proof. We begin by noting that since $\lambda \in H(P_j)$, there must exist a function $f \in \mathscr{L}(\lambda e_j)$ with $(f)_\infty = \lambda P_j$, implying that $-v_{P_j}(f) = \lambda$. Furthermore, since $\mu \in H_\iota(P_j)$, there exists a function $g \in \mathscr{L}(\iota)$ with $-v_{P_j}(g) = \mu$. We therefore obtain

$$-v_{P_j}(f^q g) = -(q v_{P_j}(f) + v_{P_j}(g)) = \mu + q\lambda = \iota_j + 1, \tag{2.20}$$

where the last equality holds by assumption. By this assessment and the definition of Riemann-Roch spaces, we have

$$(f^q g) \geq -P_j - \sum_{k=1}^{n} \iota_k P_k = -\sum_{k=1}^{n} (\iota + e_j)_k P_k,$$

which implies that $f^q g \in \mathscr{L}(\iota + e_j)$. This and equation (2.20) together imply that $f^q g \in \mathscr{L}(\iota + e_j) \setminus \mathscr{L}(\iota)$. □

Next, we show that $(\iota, \iota + e_j)$ is necessarily negligible if $\deg \iota$ is sufficiently large.

Proposition 2.4.4:
Given $\iota \in \mathbb{Z}^n$ and an integer $1 \leq j \leq n$ then $(\iota, \iota + e_j)$ is negligible when $\deg \iota \geq (q+2)(g+1) - 3$.

Proof. At first, notice that

$$\deg \iota \geq (q+2)(g+1) - 3 = qg + q + 2g - 1 \geq 2g - 1,$$

thus by the Riemann-Roch theorem 1.1.11 we have $\mathscr{L}(\iota) \subsetneq \mathscr{L}(\iota + e_j)$, since the dimension of $\mathscr{L}(\iota + e_j)$ must necessarily have increased compared to $\mathscr{L}(\iota)$ due to the size of the degree of ι. We therefore need to show that $\mu + q\lambda = \iota_j + 1$ for some non-zero $\lambda \in H(P_j)$ and some $\mu \in H_\iota(P_j)$. Recall that we can always find a non-zero $\lambda \in H(P_j)$ such that $\lambda \leq g + 1$. Now consider $\iota + (1 - q\lambda)e_j$ and its degree

$$\deg(\iota + (1 - q\lambda)e_j) \geq (qg + q + 2g - 1) + (1 - q(g+1)) = 2g.$$

Note that $\deg(\iota - q\lambda e_j) \geq 2g-1$. By the Riemann-Roch theorem 1.1.11 we thus have $\ell(\iota+(1-q\lambda)e_j) = \deg(\iota+(1-q\lambda)e_j)+1-g$ and $\ell(\iota-q\lambda e_j) = \deg(\iota-q\lambda e_j)+1-g$. Now since $\ell(\iota+(1-q\lambda)e_j) \leq \ell(\iota-q\lambda e_j)+1$, and the difference between the degrees of the two divisors is exactly 1 by design, we have $\ell(\iota+(1-q\lambda)e_j) = \ell(\iota-q\lambda e_j)+1$, hence $\mathscr{L}(\iota+(1-q\lambda)e_j) \supsetneq \mathscr{L}(\iota - q\lambda e_j)$. Therefore, there must exist some function $z \in \mathscr{L}(\iota + (1-q\lambda)e_j)$ such that $-v_{P_j}(z) = \iota_j + 1 - q\lambda$. By definition 2.4.1 we have $\iota_j + 1 - q\lambda =: \mu \in H_\iota(P_j)$, and we now obtain $\mu + q\lambda = (\iota_j + 1 - q\lambda) + q\lambda = \iota_j + 1$, hence $(\iota, \iota + e_j)$ is negligible. □

We are now prepared to formulate the bound presented by Beelen and Ruano. For this purpose, we let $M \coloneqq (q+2)(g+1) - 3$ which was the lower bound shown in proposition 2.4.4.

Theorem 2.4.5 (Beelen-Ruano Bound):
Let $F/\mathbb{F}_q$ be a function field and let $\{\iota^{(k)}\}_{-1\leq k\leq M}$ be a sequence of n-tuples satisfying $\deg \iota^{(-1)} = -1$ and that for any $0 \leq k \leq M$ there is a j such that $\iota^{(k)} - \iota^{(k-1)} = e_j$. Then $N(F)$ satisfies

$$N(F) \leq n + \sum_{k=0}^{M} \delta\left(\iota^{(k-1)}, \iota^{(k)}\right).$$

Proof. Notice that

$$1 = \deg e_j = \deg(\iota^{(k)} - \iota^{(k-1)}) = \deg \iota^{(k)} - \deg \iota^{(k-1)},$$

thus $\deg \iota^{(k)} = \deg \iota^{(k-1)} + 1$ for all $0 \leq k \leq M$. Since $\deg \iota^{(-1)} = -1$ by assumption, we have that $\deg \iota^{(k)} = k$ for all $-1 \leq k \leq M$. We also introduce a slightly modified notion of AG codes. Let thus

$$\mathcal{C}_\Psi(G) \coloneqq \left\{ \big(z(P)\big)_{P\in\Psi} : z \in \mathscr{L}(G) \right\} \subseteq \mathbb{F}_q^{N(F)-n},$$

be an algebraic geometry code where $G \in \mathrm{Div}(F)$ and Ψ is the $N(F)-n$ remaining rational places of F. It should be mentioned that the support of G must still be disjoint from $D_\Psi \coloneqq \sum_{P\in\Psi} P$. We also adopt the notation $\mathcal{C}_\Psi(\iota)$ simply to mean $\mathcal{C}_\Psi(D_\iota)$.

We will prove the result through three separate steps:

i. $\mathcal{C}_\Psi(G) = \mathbb{F}_q^{N(F)-n}$ for any $G \in \mathrm{Div}(F)$ with $\deg G \geq N(F) - n + 2g - 1$.

ii. $\dim(\mathcal{C}_\Psi(\iota^{(k)}) \leq \dim(\mathcal{C}_\Psi(\iota^{(k-1)}) + \delta(\iota^{(k-1)}, \iota^{(k)})$ for any $k \geq 0$.

iii. $\dim(\mathcal{C}_\Psi(\iota^{(-1)}) = 0$.

We begin with *i.* Recall that algebraic geometry codes are defined as the image of the evaluation map $\mathrm{ev}\colon \mathscr{L}(G) \to \mathbb{F}_q^n$ given by $z \mapsto (z(P_1), \ldots, z(P_n))$. The statement in step *i.* thus corresponds to showing surjectivity of ev. By the assumption that $\deg G \geq N(F) - n +$

$2g-1$, we now obtain

$$\begin{aligned}\dim(\mathcal{C}_\Psi(G)) &= \ell(G) - \ell(G - D_\Psi) \\ &= (\deg G + 1 - g) - (\deg G - \deg D_\Psi + 1 - g) \\ &= \deg D_\Psi \\ &= N(F) - n,\end{aligned}$$

with the first equality following from [Stichtenoth, 2009; Theorem 2.2.2] and the second from the Riemann-Roch theorem 1.1.11.

For step *ii.*, we first consider the case where $\delta(\iota^{(k)}, \iota^{(k-1)}) = 1$. Then the inequality follows directly, since we know that

$$\ell(\iota^{(k)}) \leq \ell(\iota^{(k-1)}) + 1.$$

Thus, we consider the case where $\delta(\iota^{(k)}, \iota^{(k-1)}) = 0$. By assumption we have $\iota^{(k)} = \iota^{(k-1)} + e_j$ for some $1 \leq j \leq n$. We then have by lemma 2.4.3 that there exist functions $f \in \mathscr{L}(\lambda e_j)$, with $\lambda > 0$, and $g \in \mathscr{L}(\iota^{(k-1)})$ such that $f^q g \in \mathscr{L}(\iota^{(k)}) \setminus \mathscr{L}(\iota^{(k-1)})$. This implies that $\mathcal{C}_\Psi(\iota^{(k)})$ is generated by the elements in $\mathcal{C}_\Psi(\iota^{(k-1)})$ as well as $\mathrm{ev}(f^q g)$. Note, however, that $\mathrm{ev}(f^q g) = \mathrm{ev}(fg)$ since the code is defined over $\mathbb{F}_q$. Moreover, since $\lambda > 0$, we have that $fg \in \mathscr{L}(\iota^{(k-1)})$, hence we must have $\mathrm{ev}(fg) \in \mathcal{C}_\Psi(\iota^{(k-1)})$, and consequently the dimensions must agree.

Finally, for step *iii.*, recall that $\ell(G) = 0$ if $\deg G < 0$. Then the step follows immediately, since $\deg \iota^{(-1)} = -1$.

To finish the proof, we first apply steps *ii.* and *iii.* to obtain the following inequality

$$\begin{aligned}\dim(\mathcal{C}_\Psi(\iota^{(M)})) &\leq \dim(\mathcal{C}_\Psi(\iota^{(M-1)})) + \delta(\iota^{(M-1)}, \iota^{(M)}) \\ &\leq \dim(\mathcal{C}_\Psi(\iota^{(M-2)})) + \delta(\iota^{(M-2)}, \iota^{(M-1)}) + \delta(\iota^{(M-1)}, \iota^{(M)}) \\ &\vdots \\ &\leq \dim(\mathcal{C}_\Psi(\iota^{(-1)})) + \sum_{k=0}^{M} \delta(\iota^{(k-1)}, \iota^{(k)}) \\ &= \sum_{k=0}^{M} \delta(\iota^{(k-1)}, \iota^{(k)}).\end{aligned} \tag{2.21}$$

Furthermore, by proposition 2.4.4, we clearly have that $(\iota^{(M)}, \iota^{(M)} + e_j)$ is negligible for any j since $\deg \iota^{(M)} = M$, so once again steps *ii.* and *iii.* imply that

$$\dim(\mathcal{C}_\Psi(\iota^{(M)}) = \dim(\mathcal{C}_\Psi(\iota^{(M)} + l e_j)) \tag{2.22}$$

for any j and any natural number l. We can then choose l such that $\deg(\iota^{(M)} + l e_j) \geq N(F) - n + 2g - 1$. Hence, by step *i.* and equation (2.22), we obtain

$$\dim(\mathcal{C}_\Psi(\iota^{(M)}) = N(F) - n,$$

and combining this with (2.21), one obtains the desired result. □

Remark. From proposition 2.4.4 we actually obtain a stronger bound than M. If λ_j denotes the smallest non-zero element in $H(P_j)$, then $(\iota, \iota + e_j)$ is negligible whenever $\deg \iota \geq q\lambda_j + 2g - 1$. This follows from the proof where we obtain the desired result from the fact that $\deg(\iota + (1 - q\lambda)e_j) \geq 2g$. But this can be rewritten as $\deg \iota \geq q\lambda + 2g - 1$. Thus, we shall always use this in practice.

Notice that the proof of theorem 2.4.5 is more or less a direct generalisation of the proof of theorem 2.3.2 from one rational place to n rational places. In the proof of theorem 2.3.2 we considered AG-codes of the form $\mathcal{C}_{\mathscr{L}}(D, G)$ where $D = P_1 + \cdots + P_{N-1}$ is the sum of all of the rational places except for one, and $G = tP$ where P is the last rational place. We considered a sequence of codes $\mathcal{C}_{-1}, \mathcal{C}_0, \ldots$, here using the notation $\mathcal{C}_t = \mathcal{C}_{\mathscr{L}}(D, tP)$, where $\dim(\mathcal{C}_{-1}) = 0$ and $\dim(\mathcal{C}_t) = N - 1$ for t large enough. We showed that $\dim(\mathcal{C}_t) = \dim(\mathcal{C}_{t-1}) + 1$ if and only if $t \neq \lambda_i q + \lambda$. On the other hand, for theorem 2.4.5, we treated AG-codes of the form $\mathcal{C}_\Psi(\iota^{(k)}) \coloneqq \mathcal{C}_{\mathscr{L}}(D_\Psi, D_{\iota^{(k)}})$, where D_Ψ is the sum of all of the rational places except for n places, and $D_{\iota^{(k)}} = \sum_{j=1}^{n} \iota_j^{(k)} P_j$ where $P_1, \ldots, P_n$ are the remaining n rational places. We considered a sequence of codes $\mathcal{C}_{-1}, \mathcal{C}_0, \ldots$, here using the notation $\mathcal{C}_k = \mathcal{C}_\Psi(\iota^{(k)})$ where, similar to the former proof, we obtained $\dim(\mathcal{C}_{-1}) = 0$ and $\dim(\mathcal{C}_k) = N - n$ for k large enough. We showed that $\dim(\mathcal{C}_k) \leq \dim(\mathcal{C}_{k-1}) + \delta(\iota^{(k-1)}, \iota^{(k)})$ where $\delta(\iota^{(k-1)}, \iota^{(k)}) = 1$ implies that $k \neq \lambda_j q\mu$ with $\mu \in H_\iota(P_j)$. Now, letting $n = 1$, there is only one possible sequence of codes $\mathcal{C}_k$, namely the sequence used in the proof of theorem 2.3.2. Applying this sequence throughout the above arguments, it should be clear that the Beelen-Ruano bound reduces to the Geil-Matsumoto bound for $n = 1$.

We examine how to compute the bound given in theorem 2.4.5 when $n > 1$. The requirement that our sequence of $\iota^{(k)}$ must satisfy $\iota^{(k)} = \iota^{(k-1)} + e_j$ for some j can be nicely related to graph theory. Letting a set of vertices be defined by $\{-1, 0, \ldots, M\}^n$ and edges be given as $(\iota, \iota + e_j)$ for $1 \leq j \leq n$, we obtain an n-dimensional directed graph. A simple example can be seen in figure 2.5. We make the graph weighted by assigning to each edge $(\iota, \iota + e_j)$ the weight $w(\iota, \iota + e_j) \coloneqq \delta(\iota, \iota + e_j)$. An optimal sequence $\iota^{(-1)}, \ldots, \iota^{(M)}$ can then be obtained by finding a minimum weighted path from a point of degree -1 to a point of degree M. Such a path can be obtained with Dijkstra's algorithm [Dijkstra et al., 1959]. We will showcase an example of this procedure in the following chapter.

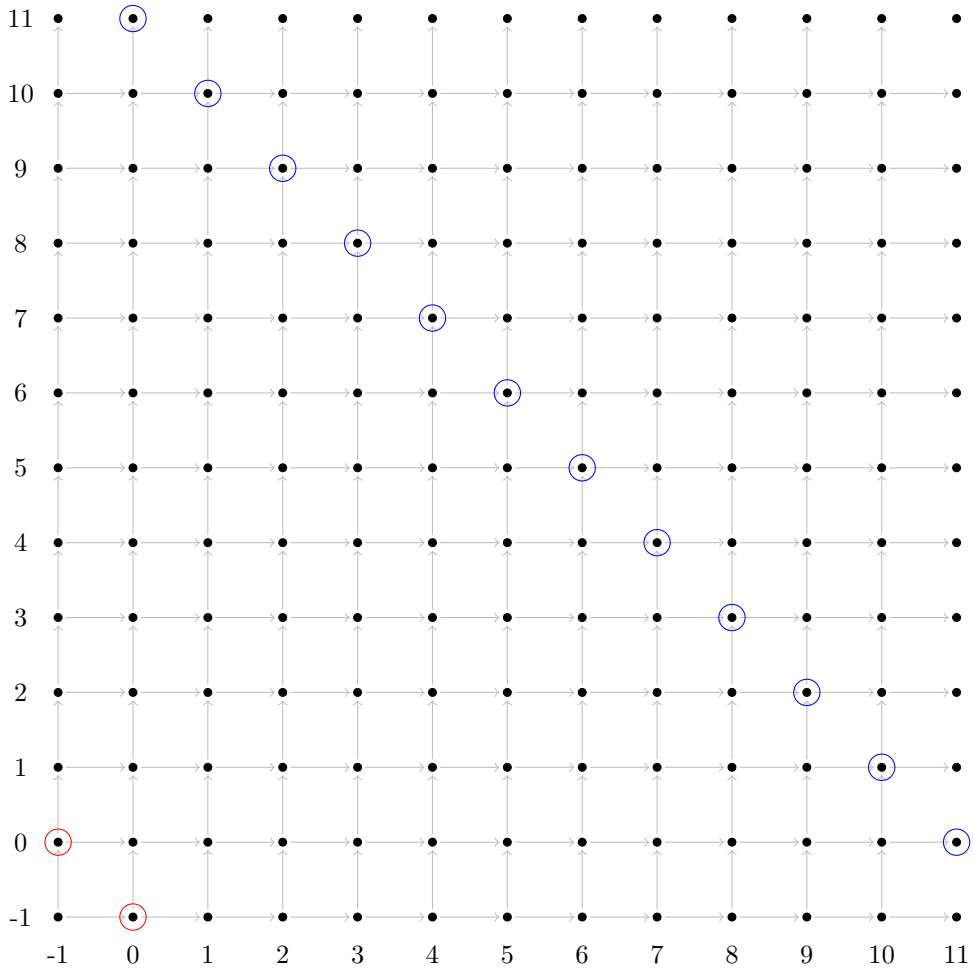

Figure 2.5: Example of directed graph for $n = 2$ and $M = 11$. Red circles represent potential starting points and blue circles represent potential ending points.

We note that a further generalisation of the Geil-Matsumoto bound is possible, using certain subsets of Ψ, however we will not cover this work. The interested reader can find more on this in [Beelen et al., 2013; §3].

Chapter 3

Application of Bounds

In the previous chapter, we examined several different bounds on the number of rational places of function fields. The first bounds only depended on the values of q and g, and the Lewittes' bound added the application of a pole number of some rational place. We expanded upon the idea of using knowledge of pole numbers by introducing the Geil-Matsumoto, in which we require information about an entire Weierstraß semigroup of some rational place. Lastly, we examined how this could be further generalised by inspecting a generalised form of pole numbers and their respective generalised Weierstraß semigroups. Having covered many of the theoretical properties of these bounds, we now seek to apply them in a slightly more practical setting.

In this chapter, we present different families of algebraic function fields as well as some of their known properties, such as genus, Weierstraß semigroups and the exact number of rational places, if these objects and values are known for the given function field. We then proceed to apply the different bounds in order to approximate N with different methods, and then compare the results. Note that one might equivalently examine corresponding algebraic curves, should one prefer a geometric approach for the application of the bounds. An overview of the correspondence between algebraic function fields and algebraic curves is given in [Stichtenoth, 2009; Appendix B]. A more rigorous treatment of algebraic curves can be found in [Tsfasman et al., 1991].

3.1 Elliptic and Hyperelliptic Function Fields

We begin by defining elliptic function fields in accordance with the definition given in [Silverman, 2009].

Definition 3.1.1:
*An **elliptic function field** is a function field $\mathcal{E} = \mathbb{F}_q(x, y)/\mathbb{F}_q$ of genus $g = 1$ such that $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$ for $a_i \in \mathbb{F}_q$, $i = 1, \ldots, 6$.*

Remark. The reader should be aware that we omit some geometric details. The reader may find useful clarification in [Silverman, 2009; Chapter 3], should they want an insight into the geometry of such function fields and their corresponding algebraic curves. Elliptic curves possess some interesting algebraic qualities. Although one most commonly interprets an elliptic curve as a locus in the plane of a cubic equation, one can define a composition that

forms an abelian group together with the curve $\mathcal{E}$. This composition allows addition of points on the curve in an algebraically meaningful way. This is, amongst other places, useful in cryptography, see for example [Hoffstein et al., 2014; Chapter 5].

Suppose that $P \in \mathbb{P}_{\mathcal{E}}$ is a rational place of an elliptic function field. By the Weierstraß Gap Theorem 1.2.3, we have $|\mathbb{N}_0 \setminus H(P)| = g = 1$, and since $1 \notin H(P)$ for any rational place, the Weierstraß semigroup of P must be generated by $\langle 2, 3\rangle$.

Serre derived the exact number of rational places of function fields of genus $g = 1$ in [Serre, 1982; Theorem 2]. We state the result.

Proposition 3.1.2:
Let $F/\mathbb{F}_q$ with $q = p^n$ be a function field of genus $g = 1$ and let $m = \lfloor 2\sqrt{q} \rfloor$. Then

$$N(F) = q + m + 1,$$

unless $p|m$ and n is odd and larger than 3, in which case

$$N(F) = q + m.$$

Proposition 3.1.2 thus states, that function fields of genus $g = 1$ meet the Serre bound, when $p \nmid m$ or $n \leq 3$.

In order to evaluate the strength of the bounds of chapter 2 on elliptic function fields, we give an example.

Example 3.1.3:
Consider $q_1 = 4$ and $q_2 = 128$ and suppose that there exist two elliptic function fields over $\mathbb{F}_4$ and $\mathbb{F}_{128}$, respectively. Then $m_1 = \lfloor 2\sqrt{q_1} \rfloor = 4$ and similarly $m_2 = 22$. Proposition 3.1.2 yields $N_1 = 9$, and it yields $N_2 = 150$ since $p_2 = 2|m_2$ and $n_2 = 7$, thus the second equation in proposition 3.1.2 applies. Note that we do not require the knowledge of the equations that defines the function fields, if we are only interested in determining the number of rational places. Of course, should we want to explicitly determine the places, then we would need the equations. Thus, in our case, we can quite conveniently apply Serre's result in order to obtain the precise number of rational places. In comparison, we apply the Lewittes bound to both cases. For the first function field we obtain $L_4(\Lambda) = 9$, which agrees with the exact number. For the other function field, we compute $L_{128}(\Lambda) = 257$, a drastic overstatement. We compute the Geil-Matsumoto bound for both function fields as well. Since the Weierstraß semigroup of any rational place has two generators, we can use the method described in theorem 2.3.12. Notice, however, that for both cases that $q_i \leq \lfloor \frac{q_i}{\lambda_1} \rfloor \lambda_2$, thus the bound agrees with the Lewittes bound. Indeed, computing the bound yields $GM_4(\Lambda) = 9$ and $GM_{128}(\Lambda) = 257$. In fact, for elliptic function fields, the Lewittes and Geil-Matsumoto bounds always agree. To see this, recall that $\Lambda = \langle 2, 3\rangle$. We see that $q \leq \lfloor \frac{q}{2} \rfloor \cdot 3$ for all $q \geq 2$. When q is even, we have $\lfloor \frac{q}{2} \rfloor \cdot 3 = \frac{3}{2}q > q$, and when $q = 2k + 1$ we have $\lfloor \frac{q}{2} \rfloor \cdot 3 = 3k$. We clearly see that $2k + 1 \leq 3k$ for all $k \in \mathbb{N}$. ◁

Elliptic function fields are a special case of so-called hyperelliptic function fields. The following is from [Best et al., 2020].

Definition 3.1.4:
*Let $\mathbb{F}_q$ have odd characteristic, and let $f(x) \in \mathbb{F}_q[x]$ be a separable polynomial, where $\deg f(x) = n > 4$ with $n = 2g + 1$ or $n = 2g + 2$. Then a **hyperelliptic function field** is a function field $F_q(x, y)/\mathbb{F}_q$ of genus g such that $y^2 = f(x)$.*

Remark. There is an alternative definition of hyperelliptic function fields that allows field characteristic 2, however we do not concern ourselves with that. Furthermore, it can be shown that if $\deg(f(x)) = 2g + 2$, then the case reduces to that of $\deg(f(x)) = 2g + 1$ (see for instance [Shafarevich, 2013; §1.4]). Finally, the notion of separability can in our case be exchanged for irreducibility, since finite fields are perfect [Brzeziński, 2018; Theorem 8.1].

Notice that determining the generators of Weierstraß semigroups for some rational place of a hyperelliptic function is not as simple as in the case of elliptic function fields. The primary issue is that x and y might have multiple poles, in which case we cannot obtain pole numbers from them the way we have defined pole numbers in this report. Therefore, we omit further theoretical discussion of Weierstraß semigroups for places of hyperelliptic function fields. Instead we give an example, where we compute the semigroup using Magma [Bosma et al., 1997]. The code used for the example can be found in appendix B.3.

Example 3.1.5:
Consider the function field $\mathbb{F}_q(x, y)/\mathbb{F}_q$ given by the equation $y^2 = f(x)$ with $f(x) = x^6 + 4x^4 + 3x^2 + 1$, and let $q = 5$. Since $\deg f(x) = 6$, we have $g = 2$. From the tables in [Geer et al., 2009] we get that this function field has 12 rational places. Indeed we obtain 12 rational places from our computations in Magma. Using the Serre bound, we denote by $S_q(g)$ the value obtained from theorem 2.1.5 and compute $S_5(2) = 14$. By further Magma computations, we obtain the gap numbers $\{1, 2\}$ of one of the rational places, say P, of our function field. Thus, we have the Weierstraß semigroup $\Lambda \coloneqq H(P) = \langle 3, 4, 5\rangle$. The Lewittes and Geil-Matsumoto bounds now yield $L_5(\Lambda) = GM_5(\Lambda) = 16$.

Consider now the polynomial $h(x) = x^6 + 1$ and the associated function field $\mathbb{F}_q(x, y)/\mathbb{F}_q$ with $q = 25$. As we still have $g = 2$, we obtain $S_{25}(2) = 46$, which is the exact number of rational places of this function field, as seen in [Geer et al., 2009]. This is of course also the output of the Hasse-Weil bound, as q is a square. Thus, this function field is $\mathbb{F}_q$-maximal. However, the other two bounds are still weaker, and they still provide the same bound, namely $L_{11}(\Lambda) = GM_{11}(\Lambda) = 34$. Thus, although hyperelliptic function fields are not generally maximal, it occurs in some cases. ◁

3.2 Hermitian and Norm-trace Function Fields

We now take a closer look at a class of function fields that has already occurred several times in the thesis. Despite having already used them on several occasions, we formally define Hermitian function fields.

Definition 3.2.1:
*A **Hermitian function field** is given by $\mathbb{F}_{q^2}(x,y)/\mathbb{F}_{q^2}$ such that $y^q + y = x^{q+1}$.*

We summarise some useful properties of Hermitian function fields, which are taken from [Stichtenoth, 2009; Lemma 6.4.4].

Proposition 3.2.2:
The Hermitian function field satisfies

i. $g = \frac{q(q-1)}{2}$.
ii. $N = q^3 + 1$.
iii. $H(P_\infty) = \langle q, q+1 \rangle$ *where P_∞ is the unique common pole of x and y.*

We have already established earlier in the thesis that Hermitian function fields are maximal both in the usual sense, but also in regard to the Geil-Matsumoto bound. In fact, the Hermitian function field is the only maximal function field over the constant field $\mathbb{F}_{q^2}$ that has genus $g = \frac{q(q-1)}{2}$, up to isomorphism. Specifically, it can be shown that for any function field $F/\mathbb{F}_{q^2}$ with genus $g = \frac{q(q-1)}{2}$ there exist $x, y \in F$, satisfying the equation $y^q + y = x^{q+1}$, such that $F = \mathbb{F}_{q^2}(x,y)$, see the theorem in [Rück et al., 1994]. Furthermore, it holds for any maximal function field that every subfield with the same base field is maximal as well, see [Lachaud, 1987; Proposition 6]. Thus, it makes sense to find subfields of the Hermitian function field in order to obtain additional maximal function fields. Since the full automorphism group of the Hermitian function field is well studied and known to be large, it may lead to many maximal subfields. In fact, if $\mathcal{H}_q$ denotes the Hermitian function field, then it is known that $|\mathrm{Aut}(\mathcal{H}_q)| = (q^3+1)q^3(q^2-1)$, see [Leopoldt, 1996].

One may ask oneself if it should not also be possible to define function fields based on a similar premise for arbitrary exponents on q. We therefore examine a generalisation of these function fields. The following definition is from [Brzeziński, 2018].

Definition 3.2.3:
*Consider a field extension L/K and suppose it is Galois with Galois group $G = \mathrm{Gal}(L/K)$. Then the **norm** and **trace** functions are maps $\mathcal{N}\colon L \to K$ and $\mathcal{T}\colon L \to K$, respectively, given by*

$$\mathcal{N}(\alpha) = \prod_{\sigma \in G} \sigma(\alpha), \qquad \mathcal{T}(\alpha) = \sum_{\sigma \in G} \sigma(\alpha).$$

Specifically, we are interested in the norm and trace on finite fields. Consider first the field $\mathbb{F}_q$. Letting $r \geq 1$, the extension $\mathbb{F}_{q^r}/\mathbb{F}_q$ is Galois and of degree r. Its Galois group is a cyclic

group generated by the so-called *Frobenius automorphism* $\varphi\colon \mathbb{F}_{q^r} \to \mathbb{F}_q$ given by $\varphi(\alpha) = \alpha^q$. We thus obtain

$$\mathcal{N}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) = \prod_{k=0}^{r-1} \alpha^{q^k} = \alpha^{\frac{q^r-1}{q-1}}, \qquad \mathcal{T}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(\alpha) = \sum_{k=0}^{r-1} \alpha^{q^k} = \alpha + \alpha^q + \cdots + \alpha^{q^{r-1}},$$

for $\alpha \in \mathbb{F}_{q^r}$ [Stichtenoth, 2009; §A.15]. This motivates the following definition, as introduced in [Geil, 2003].

Definition 3.2.4:
*A **norm-trace function field** is a function field $\mathbb{F}_{q^r}(x,y)/\mathbb{F}_{q^r}$ with $r \geq 2$ such that*

$$\mathcal{N}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(x) = \mathcal{T}_{\mathbb{F}_{q^r}/\mathbb{F}_q}(y).$$

Note that $\mathcal{N}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(x) = x^{q+1}$ and $\mathcal{T}_{\mathbb{F}_{q^2}/\mathbb{F}_q}(y) = y + y^q$. Thus, for $r = 2$, definition 3.2.4 simply reduces to Hermitian function fields.

We summarise some generalised results for norm-trace function fields, which are found in [Geil, 2003] and [Munuera et al., 2008].

Proposition 3.2.5:
The norm-trace function field satisfies

i. $g = (q^{r-1}-1)(\frac{q^r-1}{q-1}-1)/2$.
ii. $N = q^{2r-1}+1$.
iii. $H(P_\infty) = \langle q^{r-1}, \frac{q^r-1}{q-1}\rangle$ *where P_∞ is the unique common pole of x and y.*

We examine the precision of the bounds from chapter 2 on norm-trace function fields.

Example 3.2.6:
Let $q = 2$ and $r = 3$ and consider the function field $\mathbb{F}_8(x,y)/\mathbb{F}_8$ that satisfies $x^7 = y+y^2+y^4$. Then by proposition 3.2.5 we obtain $g = 9$. Likewise, we know that the exact number of rational places of this function field is $N = 33$, and it has a rational place whose Weierstraß semigroup is $\Lambda = \langle 4, 7\rangle$. We begin by applying the Serre bound. Note, however, that the q used in $S_q(g)$ as well as in $L_q(\Lambda)$ and $GM_q(\Lambda)$ refers to the number of elements in the constant field, in this case 8. We obtain $S_8(9) = 54$. Since our alphabet size is not a square, this cannot be a maximal function field. Computing the Lewittes and Geil-Matsumoto bounds, we obtain $L_8(\Lambda) = GM_8(\Lambda) = 33$. Thus, this function field is still maximal in the sense of the Geil-Matsumoto bound. Note that, once again, these two bounds agree. To examine this occurrence, recall proposition 2.3.17. Since Λ is generated by two elements, we know that $L_q(\Lambda) = GM_q(\Lambda)$ if and only if $q \leq \lfloor \frac{q}{\lambda_1} \rfloor \lambda_2$. From proposition 3.2.5 we have $\lambda_1 = q^{r-1}$ and $\lambda_2 = \frac{q^r-1}{q-1}$. We then see that $\lfloor \frac{q}{\lambda_1} \rfloor \lambda_2 = \lfloor \frac{q}{q^{r-1}} \rfloor \lambda_2 = \lambda_2$ for all $r \geq 2$. Since we clearly always have $q \leq \lambda_2 = \frac{q^r-1}{q-1}$ for $r \geq 2$, $L_q(\Lambda)$ and $GM_q(\Lambda)$ will always agree.

As a second example, consider what happens to the original set-up, if we let $r = 4$. Then we have alphabet size 16, genus $g = 49$, exactly $N = 129$ rational places and $\Lambda = \langle 8, 15\rangle$.

As expected, we have $L_{16}(\Lambda) = GM_{16}(\Lambda) = 129$, and from the Serre bound, and the Hasse-Weil bound for that matter, we obtain $S_{16}(49) = 409$. Thus, norm-trace function fields are generally not maximal in the classical sense. They do, however, have the largest possible number of rational places given their specific Weierstraß semigroup. This is also easily verified by the fact that $L_{q^r}(\Lambda) = q^r\lambda_1 + 1 = q^{2r-1} + 1 = N$ and by the earlier arguments that $L_q(\Lambda) = GM_q(\Lambda)$. ◁

3.3 Suzuki Function Fields

We examine another family of function fields that is in some sense related to the Hermitian function fields. The following is based on [Bartoli et al., 2021b].

Definition 3.3.1:
*A **Suzuki function field** is a function field $\mathbb{F}_q(x, y)/\mathbb{F}_q$ such that $y^q + y = x^{q_0}(x^q + x)$ where $q = 2q_0^2$, $q_0 = 2^h$, $h > 0$.*

The following summary of known properties of the Suzuki function field is from [Matthews, 2004] and [Stichtenoth et al., 1990].

Proposition 3.3.2:
Let $\mathcal{S}_q$ be a Suzuki function field, and let $P \in \mathbb{P}_{\mathcal{S}}$ be rational. Then

i. $H(P) = \langle q, q + q_0, q + 2q_0, q + 2q_0 + 1\rangle$.
ii. $g = q_0(q - 1)$.
iii. $N(\mathcal{S}_q) = q^2 + 1$.

As previously hinted, the Suzuki function field is somewhat related to Hermitian function fields. To further explore this relation, we refer to their respective associated algebraic curves, namely the Suzuki curve and the Hermitian curve. These two classes of curves are, together with the so-called Ree curves, known collectively as the *Deligne-Lusztig curves* [Deligne et al., 1976]. These curves can all be derived from specific finite groups. The Deligne-Lusztig curves have enjoyed a lot of attention in the literature, and extensive studies have been done on all of them. Most noticeably, they are all maximal in some sense, and they all admit large automorphism groups. Therefore, they are of particular interest in coding theory. For instance, the Suzuki function field is $\mathbb{F}_{q^4}$-maximal. To see this, recall the Hasse-Weil bound

$$HW_q(g) = 2g\sqrt{q} + q + 1.$$

Let g be given as in proposition 3.3.2. We now obtain

$$HW_{q^4}(g) = 2gq^2 + q^4 + 1 = 2q_0(q - 1)q^2 + q^4 + 1,$$

which is shown to be the exact number of rational places of the Suzuki function field over $\mathbb{F}_{q^4}$ in [Eid et al., 2014]. Furthermore, it is *optimal* over $\mathbb{F}_q$, meaning it has the maximum possible number of rational places over $\mathbb{F}_q$ [Stichtenoth et al., 1990; Proposition 2.1].

The Suzuki function field also admits a large automorphism group. Specifically, it is known that $|\mathrm{Aut}(\mathcal{S}_q)| = (q^2+1)q^2(q-1)$. Moreover, similarly to Hermitian function fields, one can show that every function field of genus $g = q_0(q-1)$ and with $N = q^2+1$ is isomorphic to a Suzuki function field [Eid et al., 2014; Proposition 2.1]. Going further into this topic, however, gets very involved and deep, and we will thus not look further into it.

Example 3.3.3:
Let $h = 1$, thus $q_0 = 2$ and $q = 8$. Consider $\mathbb{F}_8(x,y)/\mathbb{F}_8$ such that $y^8 + y = x^{10} + x^2$. Then by proposition 3.3.2 this function field has a rational place with Weierstraß semigroup generated by $\{8, 10, 12, 13\}$. This yields the numerical semigroup

$$\Lambda = \{0, 8, 10, 12, 13, 16, 18, 20, 21, 22, 23, 24, 25, 26\} \cup \{i \in \mathbb{N}_0 | i \geq 28\}$$

of genus $g = 14$. The table from [Geer et al., 2009] tells us that such a function field must have exactly 65 rational places. Applying the Serre bound, we obtain $S_8(14) = 79$.

Notice that $\lambda_1 = q$ and $\lambda_2 = q + q_0$. By way of this we have $\lfloor \frac{q}{\lambda_1} \rfloor \lambda_2 = q + q_0$. Thus, proposition 2.3.17 tells us that $L_q(\Lambda) = GM_q(\Lambda)$ for all q for this family of function fields. Indeed, both the Lewittes and the Geil-Matsumoto bounds output $L_8(\Lambda) = GM_8(\Lambda) = 65$.◁

3.4 Klein Quartics

For this last section, we take a look at a function field that was examined in an example in [Beelen et al., 2013]. Due to time constraints, we have omitted a functional implementation of the Beelen-Ruano bound from this thesis. Instead, we analyse the bound as applied in the original paper, as well as compare it to the other bounds presented in this thesis. The following is from [Hansen, 1987].

Definition 3.4.1:
The Klein quartic is a function field $\mathcal{K} = \mathbb{F}_8(x,y)/\mathbb{F}_8$ such that $x^3y + y^3 + x = 0$.

We summarise some important properties of the Klein quartic, which are taken from [Stichtenoth, 2009] and [Høholdt et al., 1998].

Proposition 3.4.2:
Let $\mathcal{K}$ be the Klein quartic and let Q be a zero or a pole of x and y. Then

i. $g = 3$.
ii. $N(\mathcal{K}) = 24$.
iii. $H(Q) = \langle 3, 5, 7 \rangle$.

Example 3.4.3:
Consider the Klein quartic with the equation $x^3y + y^3 + x = 0$. We have $q = 8$ and $g = 3$, so the Serre bound yields $S_8(3) = 24$, thus the Klein quartic is as close to maximal as can be

with this value of q. However, when testing the Lewittes and Geil-Matsumoto bounds with $\Lambda = \langle 3, 5, 7\rangle$, we obtain $L_8(\Lambda) = GM_8(\Lambda) = 25$, which was to be expected by proposition 2.3.17 since $q = 8 \leq 10 = \lfloor \frac{q}{\lambda_1} \rfloor \lambda_2$.

In [Beelen et al., 2013; Example 1], the Beelen-Ruano is applied to the Klein quartic. They compute the generalised Weierstraß semigroups of two rational places of the function field and all of the $\delta(\iota, \iota + e_j)$ in order to determine the weights in the corresponding directed graph. Note that by the remark following theorem 2.4.5, we need only consider $\iota^{(k)}$ for $k = -1, 0, \ldots, 29$, since if $\deg \iota \geq q\lambda_j + 2g - 1 = 29$, we have $\delta(\iota, \iota + e_j) = 0$. By applying Dijkstra's algorithm, they obtain a minimum weighted path given by

$$\begin{cases} \iota^{(k)} = (k, 0), & k = -1, 0, \ldots, 23, \\ \iota^{(23+k)} = (24, k-1), & k = 1, 2, 3, \\ \iota^{(26+k)} = (25, k+1), & k = 1, 2, 3. \end{cases}$$

This minimum weighted path is visualised in figure 3.1.

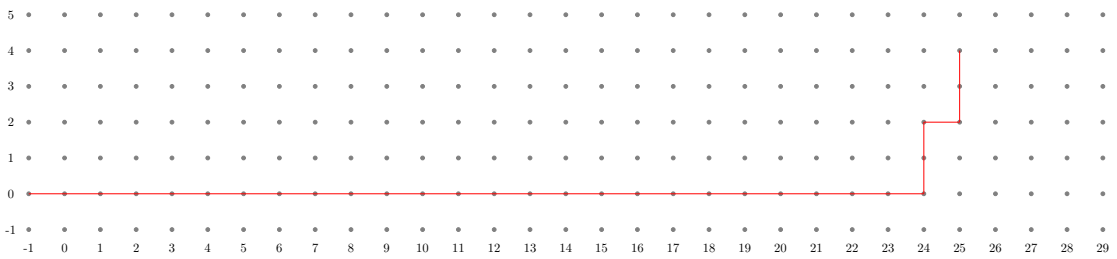

Figure 3.1: A minimum weighted path from a point of degree -1 to a point of degree 29 when applying the Beelen-Ruano bound to the Klein quartic.

They then conclude that $\{k \geq 0 : \delta(\iota^{(k-1)}, \iota^{(k)}) = 1\} = \{0, 3, 5, 6, \ldots, 23, 25\}$, so by theorem 2.4.5 they obtain $N(\mathcal{K}) \leq 24$. Thus, in this case, the Beelen-Ruano bound is stronger than the Geil-Matsumoto bound, albeit not by much. Additionally, the computation of the Beelen-Ruano bound may be more expensive in the sense of computation. ◁

References

Bartoli, Daniele, Maria Montanucci, and Fernando Torres (2021a). "$\mathbb{F}_{p^2}$*-maximal curves with many automorphisms are Galois-covered by the Hermitian curve*". In: *Advances in Geometry* 21.3, pages 325–336. DOI: doi:10.1515/advgeom-2021-0013. URL: https://doi.org/10.1515/advgeom-2021-0013.

Bartoli, Daniele, Maria Montanucci, and Giovanni Zini (2021b). "*Weierstrass semigroups at every point of the Suzuki curve*". eng. In: *Acta Arithmetica*. DOI: 10.4064/aa181203-24-2.

Beelen, Peter (2007). "*The order bound for general algebraic geometric codes*". In: *Finite Fields and Their Applications* 13, pages 665–680. DOI: 10.1016/j.ffa.2006.09.006.

Beelen, Peter and Diego Ruano (2013). "*Bounding the number of points on a curve usaing a generalization of Weierstraß semigroups*". In: *Designs, Codes and Cryptography* 66, pages 221–230.

Beelen, Peter and Nesrin Tutas (2006). "*A generalization of the Weierstrass semigroup*". In: *Journal of Pure and Applied Algebra* 207, pages 243–260.

Best, Alex J. et al. (2020). *A user's guide to the local arithmetic of hyperelliptic curves*. Retrieved June 3, 2022. DOI: 10.48550/ARXIV.2007.01749. URL: https://arxiv.org/abs/2007.01749.

Bosma, Wieb, John Cannon, and Catherine Playoust (1997). "The Magma algebra system. I. The user language". In: *J. Symbolic Comput.* 24.3-4. Computational algebra and number theory (London, 1993), pages 235–265. ISSN: 0747-7171. DOI: 10.1006/jsco.1996.0125. URL: http://dx.doi.org/10.1006/jsco.1996.0125.

Bras-Amorós, Maria (2008). "*Fibonacci-like behavior of the number of numerical semigroups of a given genus*". In: *Semigroup Forum, Springer* 76.2, pages 379–384.

Bras-Amorós, Maria and Albert Vico-Oton (2014). "*On the Geil-Matsumoto Bound and the Length of AG Codes*". In: *Designs, Codes and Cryptography, Springer* 70.1-2, pages 117–125.

Brzeziński, Juliusz (2018). *Galois Theory Through Exercises*. eng. Cham.

COS++ (2021). *The Combinatorial Object Server: Generate numerical semigroups*. Retrieved June 3, 2022. URL: http://combos.org/sgroup.

Deligne, P. and G. Lusztig (1976). "*Representations of Reductive Groups Over Finite Fields*". In: *Annals of Mathematics* 103.1, pages 103–161. ISSN: 0003486X. URL: http://www.jstor.org/stable/1971021 (visited on 05/24/2022).

Dijkstra, Edsger W., Laurent Beauguitte, and Marion Maisonobe (1959). "*A Note on Two Problems in Connexion with Graphs*". fre. In: *Numerische Mathematik* 1, pages 269–271.

Eid, Abdulla et al. (2014). *Suzuki-invariant codes from the Suzuki curve*. DOI: 10.48550/ARXIV.1411.6215. URL: https://arxiv.org/abs/1411.6215.

Geer, Gerard van der et al. (2009). *Tables of Curves with Many Points*. Retrieved June 3, 2022. URL: http://www.manypoints.org.

Geil, Olav (2003). "*On codes from norm–trace curves*". eng. In: *Finite fields and their applications* 9.3, pages 351–371. ISSN: 1071-5797.

Geil, Olav and Ryutaroh Matsumoto (2009). "*Bounding the number of $\mathbb{F}_q$-rational places in algebraic function fields using Weierstrass semigroups*". In: *Journal of Pure and Applied Algebra* 213, pages 1152–1156.

Hansen, Johan P. (1987). "*Codes on the Klein quartic, ideals, and decoding*". English. In: *I E E E Transactions on Information Theory* 33.6, pages 923–925. ISSN: 0018-9448.

Hirschfeld, J. W. P., G. Korchmáros, and F. Torres (2013). *Algebraic Curves over a Finite Field*. Princeton University Press. ISBN: 9781400847419. DOI: doi:10.1515/9781400847419.

Hoffstein, Jeffrey, Jill Pipher, and Joseph H Silverman (2014). *An Introduction to Mathematical Cryptography*. eng. Undergraduate texts in mathematics. New York, NY: Springer New York. ISBN: 9780387779935.

Høholdt, T., J. Lint, and R. Pellikaan (1998). "*Algebraic geometry of codes, handbook of coding theory*". In: *Amsterdam*, pages 871–961.

Lachaud, Gilles (Jan. 1987). "*Sommes d"Eisenstein et nombre de points de certaines courbes alg'ebriques sur les corps finis*". In: *C. R. Acad. Sci. Paris* 305.

Lauritzen, Niels (2011). *Concrete Abstract Algebra*. eng. Cambridge. ISBN: 978-0-521-53410-9.

Leopoldt, Heinrich-Wolfgang (1996). "*Über die Automorphismengruppe des Fermatkörpers*". In: *Journal of Number Theory* 56.2, pages 256–282. ISSN: 0022-314X. DOI: https://doi.org/10.1006/jnth.1996.0017. URL: https://www.sciencedirect.com/science/article/pii/S0022314X96900177.

Lewittes, Joseph (1990). "*Places of degree one in function fields over finite fields*". In: *Journal of Pure and Applied Algebra* 69, pages 177–183.

Matthews, G.L. (2004). "*Codes from the Suzuki function field*". In: *IEEE Transactions on Information Theory* 50.12, pages 3298–3302. DOI: 10.1109/TIT.2004.838102.

Munuera, Carlos, Guilherme C. Tizziotti, and Fernando Torres (2008). "Two-Point Codes on Norm-Trace Curves". In: *Proceedings of the 2nd International Castle Meeting on Coding Theory and Applications*. ICMCTA '08. Castillo de la Mota, Medina del Campo, Spain: Springer-Verlag, 128–136. ISBN: 9783540874478. DOI: 10.1007/978-3-540-87448-5_14. URL: https://doi.org/10.1007/978-3-540-87448-5_14.

R Core Team (2022). *R: A Language and Environment for Statistical Computing*. R Foundation for Statistical Computing. Vienna, Austria. URL: https://www.R-project.org/.

Rück, Hans-Georg and Henning Stichtenoth (1994). "*A characterization of Hermitian function fields over finite fields.*" In: 1994.457, pages 185–188. DOI: doi:10.1515/crll.1994.457.185. URL: https://doi.org/10.1515/crll.1994.457.185.

Serre, Jean-Pierre (1982). "*Nombres des points des courbes algébriques sur F_q*". In: *Séminaire de Théorie des Nombres de Bordeaux*. Retrieved June 3, 2022, pages 1–8. URL: http://www.jstor.org/stable/44166412.

Serre, Jean-Pierre (1983). "*Sur le nombre des points rationnels d'une courbe algébrique sur un corps fini*". In: *C. R. Acad. Sci. Paris* série I.296, pages 397–402.

Shafarevich, Igor R. (2013). *Basic Algebraic Geometry 1 : Varieties in Projective Space*. eng. -3rd ed. 2013. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 9783642379567.

Silverman, Joseph H (2009). *The Arithmetic of Elliptic Curves*. eng. 2. Aufl. New York, NY: Springer-Verlag. ISBN: 0387094938.

Stichtenoth, Henning (2009). *Algebraic Function Fields and Codes*. eng. 2nd ed. 2009. Graduate Texts in Mathematics, 254. Berlin, Heidelberg: Springer Berlin Heidelberg. ISBN: 3-540-76878-5.

Stichtenoth, Henning and Johan P. Hansen (1990). "*Group codes on certain algebraic curves with many rational points*". In: *Applicable Algebra in Engineering, Communication and Computing* 1, pages 67–77. DOI: 10.1007/BF01810849.

Tsfasman, M. A. and S. G. Vlăduţ (1991). *Algebraic-Geometric Codes*. eng. Springer Netherlands. ISBN: 0-7923-0727-5.

Appendix **A**

Details of Proofs

In this appendix we expand upon some details that were left out of proofs due to them being lengthy and technical as well as distracting the reader from the interesting parts of the proofs.

A.1 Calculations omitted in theorem 2.3.12

A lot of details are left out of equations (2.14) and (2.15). We state them here.

$$\begin{aligned}
\lambda - q\lambda_1 \notin \Lambda &\iff \lambda_2 \left((\lambda - q\lambda_1)\nu \mod \lambda_1\right) > \lambda - q\lambda_1 \\
&\iff \lambda_2 \left((m\lambda_1 + n\lambda_2 - q\lambda_1)\nu \mod \lambda_1\right) > \lambda - q\lambda_1 \\
&\iff \lambda_2 \left(n\lambda_2\nu \mod \lambda_1\right) > \lambda - q\lambda_1 \\
&\iff \lambda_2 (n \mod \lambda_1) > \lambda - q\lambda_1 \\
&\iff \lambda_2 n > (m-q)\lambda_1 + n\lambda_2 \\
&\iff 0 > (m-q)\lambda_1 \\
&\iff q > m.
\end{aligned}$$

In the first line, we apply lemma 2.3.11*ii.* In the second line, we have from lemma 2.3.11*i.* that there exist unique $m, n \in \mathbb{N}_0$ such that $\lambda = m\lambda_1 + n\lambda_2$. In the fourth line, we use that ν is the inverse of λ_2 modulo λ_1, and in the fifth line we both use lemma 2.3.11*i.* on the right hand side and the fact that $0 \leq n \leq \lambda_1 - 1$, thus $n \mod \lambda_1 = n$.

$$\begin{aligned}
\lambda - q\lambda_2 \notin \Lambda &\iff \lambda_2 \left((\lambda - q\lambda_2)\nu \mod \lambda_1\right) > \lambda - q\lambda_2 \\
&\iff \lambda_2 \left((m\lambda_1 + n\lambda_2 - q\lambda_2)\nu \mod \lambda_1\right) > \lambda - q\lambda_2 \\
&\iff \lambda_2 \left((n-q)\lambda_2\nu \mod \lambda_1\right) > \lambda - q\lambda_2 \\
&\iff \lambda_2 \left((n-q) \mod \lambda_1\right) > m\lambda_1 + (n-q)\lambda_2 \\
&\iff \lambda_2 \left(\left((n-q) \mod \lambda_1\right) - (n-q)\right) > m\lambda_1 \\
&\iff \lambda_2 \left(-\lfloor \frac{n-q}{\lambda_1} \rfloor \lambda_1\right) > m\lambda_1 \\
&\iff \lambda_2 \left(-\lfloor \frac{n-q}{\lambda_1} \rfloor\right) > m
\end{aligned}$$

$$\iff \lambda_2 \left(\lceil -\frac{n-q}{\lambda_1} \rceil \right) > m$$
$$\iff \lambda_2 \left(\lceil \frac{q-n}{\lambda_1} \rceil \right) > m.$$

Several steps are similar to those of the first case. In the sixth line, we apply the rule

$$n - q = \lambda_1 \lfloor (n-q)/\lambda_1 \rfloor + ((n-q) \mod \lambda_1).$$

Arguments for this rule are given in the proof of lemma 2.3.11.

A.2 Calculations omitted in lemma 2.3.16

We restate the final bi-implication

$$\frac{\lambda_i}{d} \left(q \mod \frac{\lambda_1}{d} \right) \leq q \left(\frac{\lambda_i}{d} - \frac{\lambda_1}{d} \right) \iff qd \leq \left\lfloor \frac{qd}{\lambda_1} \right\rfloor \lambda_i. \tag{A.1}$$

We once again use the relation

$$q = \frac{\lambda_1}{d} \left\lfloor \frac{qd}{\lambda_1} \right\rfloor + \left(q \mod \frac{\lambda_1}{d} \right),$$

to rewrite

$$\frac{\lambda_i}{d} \left(q \mod \frac{\lambda_1}{d} \right) = \frac{\lambda_i}{d} \left(q - \frac{\lambda_1}{d} \left\lfloor \frac{qd}{\lambda_1} \right\rfloor \right)$$

in (A.1). We now obtain

$$\begin{aligned} \frac{\lambda_i}{d} \left(q - \frac{\lambda_1}{d} \left\lfloor \frac{qd}{\lambda_1} \right\rfloor \right) \leq q \left(\frac{\lambda_i}{d} - \frac{\lambda_1}{d} \right) &\iff \frac{\lambda_i}{d} \left(-\frac{\lambda_1}{d} \left\lfloor \frac{qd}{\lambda_1} \right\rfloor \right) \leq q \left(-\frac{\lambda_1}{d} \right) \\ &\iff -\frac{\lambda_i}{d} \left\lfloor \frac{qd}{\lambda_1} \right\rfloor \leq -q \\ &\iff qd \leq \lambda_i \left\lfloor \frac{qd}{\lambda_1} \right\rfloor, \end{aligned}$$

as desired.

Appendix B

Scripts for Experiments

This appendix includes scripts used throughout the report, mainly for calculations in examples. All scripts are written in R [R Core Team, 2022].

B.1 Implementation of Bounds

The following code is used for the calculations of multiple examples.

```
S <- function(x,g){floor(2*sqrt(x))*g+x+1}

L <- function(x,l){x*l[1]+1}

GM <- function(x,l,L){
  cosets <- c()
  for (i in 1:length(l)){
    cosets <- c(cosets,x*l[i]+L)
  }
  Union <- unique(c(cosets,(x*l[1]+L[length(L)]):(x*l[length(l)]+L[length(
    L)])))

  L <- c(L, (L[length(L)]+1):(Union[length(Union)]))
  L <- L[!L%in% Union]

  N <- length(L) + 1; N
}

GMmod <- function(x,g){(x-1/x)*(g+1)+2}

GMBA <- function(x,l){
  if (x <= ceiling((x-l[1]+1)/l[1])*l[2]){
    N <- 1+x*l[1]
  }
  else if (ceiling((x-l[1]+1)/l[1])*l[2] < x & x < ceiling(x/l[1])*l[2]){
    N <- 1+(x%%l[1])*x+(l[1]-(x%%l[1]))*ceiling((x-l[1]+1)/l[1])*l[2]
  }
  N
}
```

Here, `S`, `L` and `GM` are the implementations of the Serre, Lewittes and Geil-Matsumoto

bounds, respectively. Additionally, `GMmod` is the bound derived from the Geil-Matsumoto bound in proposition 2.3.9, and `GMBA` is the closed form of the Geil-Matsumoto bound derived in theorem 2.3.12. For the inputs, `x` and `g` denote alphabet size and genus, respectively, where `l` denotes the generating set for the numerical semigroup `L`. Note that Lewittes' bound takes the generating set of Λ as input and uses the first entry, λ_1. One may input $g+1$ instead, if one does not know the generators of Λ.

B.2 Generation of Numerical Semigroups with Two Generators

The following code generates a numerical semigroup from two coprime integers.

```
Semi2gen <- function(l){
  L <- c()
  for (a in 0:floor((l[1]*l[2]-l[1]-l[2])/l[1])){
    for (b in 0:floor((l[1]*l[2]-l[1]-l[2])/l[2])){
      if (a*l[1]+b*l[2] <= l[1]*l[2]-l[1]-l[2]){
        L <- union(L, c(a*l[1]+b*l[2]))
      }
    }
  }
  L <- c(sort(L),l[1]*l[2]-l[1]-l[2]+1)
  r <- 0:max(L)
  g <- length(r[!r %in% L])
  list(L,g)
}
```

As in section B.1, `l` is the generating set of the numerical semigroup. The function yields two outputs, `L` and `g`, which are the numerical semigroup generated by `l` and the genus of said semigroup, respectively.

B.3 Magma code for example 3.1.5

The following code was used to compute the rational places and the gaps of the function field $\mathbb{F}_5(x,y)/\mathbb{F}_5$ given by $y^2 = x^6 + 4x^4 + 3x^2 + 1$.

```
R<X> := PolynomialRing(GF(5));
P<T> := PolynomialRing(R);
F<Y> := FunctionField(T^2-X^6-4*X^4-3*X^2-1);

P := Places(F,1);
GapNumbers(F, P[1]);
```

Here, `Places(F,n)` outputs a list containing the places of degree n of the function field F. We obtain the gaps of the rational place P of F with `GapNumbers(F, P)`, by which we can deduce the generators of $H(P)$.

Appendix C

List of Symbols

Symbol	Description
F/K	Algebraic function field F over the base field K
$[F : K]$	Degree of F/K
$\mathbb{P}_F$	Set of places of the function field F/K
$\mathcal{O}_P$	Valuation ring corresponding to the place P
$v_P(z)$	Valuation of z in the place P
$z(P)$	Evaluation of z in the place P
$\mathrm{Div}(F)$	Group of divisors of the function field F/K
$(z)_0$	Zero divisor of z
$(z)_\infty$	Pole divisor of z
(z)	Principal divisor of z
$\mathscr{L}(D)$	Riemann-Roch space of the divisor D
$\ell(D)$	Dimension of the divisor D
g	Genus of a function field
$\mathcal{A}_F$	Adele space of the function field F/K
Ω_F	Space of Weil differentials of the function field F/K
$i(D)$	Index of specialty of the divisor D
$H(P)$	Weierstraß semigroup of the place P
$\mathbb{F}_q$	Finite field with q elements
$N(F)$	Number of rational places of the function field F/K
$e(P'\|P)$	Ramification index of the place P' over the place P
$f(P'\|P)$	Relative degree of the place P' over the place P
$\mathcal{C}_{\mathscr{L}}(D, G)$	Algebraic geometry code defined by the divisors D and G
Λ	Numerical semigroup
$S_q(g)$	Serre bound computed with fixed q and g
$L_q(\Lambda)$	Lewittes bound computed with fixed q and Λ
$GM_q(\Lambda)$	Geil-Matsumoto bound computed with fixed q and Λ
$HW_q(g)$	Hasse-Weil bound computed with fixed q and g
$H_\iota(P_j)$	Quasi-generalised Weierstraß semigroup of the place P_j