ON CONGRUENCE FUNCTION FIELDS WITH MANY RATIONAL PLACES

BY

KIT HO MAK

DISSERTATION

Submitted in partial fulfillment of the requirements
for the degree of Doctor of Philosophy in Mathematics
in the Graduate College of the
University of Illinois at Urbana-Champaign, 2012

Urbana, Illinois

Doctoral Committee:

Associate Professor Hal Schenck, Chair
Associate Professor Iwan Duursma, Director of Research
Emeritus Professor Stephen Ullom
Professor Alexandru Zaharescu

Abstract

In this thesis, we study congruence function fields, in particular those with many rational places. This thesis consists of three parts, the first two parts present our results in two different aspects of function fields with many rational places, namely maximal function fields and asymptotically good towers of function fields. The third part concerns Selmer groups of elliptic curves over the rational function field.

Let $\mathcal{H}$ be the Hermitian function field, and $\mathcal{C}$ be a maximal function field, both over the same finite field. In the first part of this thesis, we analyze the Artin representation of $\mathcal{H}$ and improve the lower bound for the possible degree of the extension $\mathcal{H}/\mathcal{C}$ when it is Galois. We then apply the lower bound to show that the generalized Giulietti-Korchmáros function field defined over $\mathbb{F}_{q^{2n}}$ is not a Galois subfield of the Hermitian function field $\mathcal{H}$ over $\mathbb{F}_{q^{2n}}$ for $n \geq 3$ odd and $q \geq 3$. Combining the lower bound with some group theoretical arguments, we also generalize an example given by Garcia and Stichtenoth by showing that when q is an odd prime, the function field $\mathcal{X}_3 = \mathbb{F}_{q^6}(x, y)$ with $x^{q^2} - x = y^{(q^n+1)/(q+1)}$ is not a Galois subfield of the Hermitian function field over the same finite field.

The second part is about improving lower bounds of the Ihara constant. Let $\mathcal{X}$ be a curve over $\mathbb{F}_q$ and let $N(\mathcal{X})$, $g(\mathcal{X})$ be its number of rational places and genus respectively. The Ihara constant $A(q)$ is defined by $A(q) = \limsup_{g(\mathcal{X})\to\infty} N(\mathcal{X})/g(\mathcal{X})$. We use a variant of Serre's class field tower method to obtain an improvement of the best known lower bounds on $A(2)$ and $A(3)$.

In the last part, we calculate the distribution of Selmer groups arising from a 2-isogeny for a family of quadratic twists of the elliptic curves with full 2-torsions over the rational function field $\mathbb{F}_q(x)$ for odd q. In particular, we show that the sizes of these Selmer groups are almost always bounded. The calculation relies heavily on various estimates of twisted character sums over function fields.

To my parents.

Acknowledgments

First I would like to thank my advisor Prof. Iwan Duursma for introducing me the beautiful area of function fields over finite fields, and for all his support and guidance during the work.

My thanks to Prof. Alexandru Zaharescu for his interesting ideas that make my graduate life busy. I would also like to thank Prof. Hal Schenck and Prof. Stephen Ullom for serving on my thesis committee and discussing with me about my research.

I wish to thank my family: my mother, my father, my brother and my sister for their unconditional support, love and encouragement in my entire life.

Thanks to my officemates and the number theory students who made my graduate life more enjoyable, especially to MTip who always hit me up with interesting discussions, and to Michael, Paul and Roy for the laughters in the office. My thanks also go to the Chatown group for their numerous dinner gatherings and game nights.

Table of Contents

Chapter 1

Introduction

This is a thesis on congruence function fields, in particular those with many rational places. These function fields are interesting and have applications in coding theory [32, 67, 80, 85, 90], cryptography and secret sharing schemes [9, 11], low-discrepancy sequences [61, 62, 63, 64] and in finite geometry [43]. Two of the major themes of study of these function fields are maximal function fields, and the search of towers of function fields that have asymptotically many rational places as the genus of the tower goes to infinity. The main aim of this thesis is to present our results in both themes.

1.1 Maximal function fields

Let p be a prime, and let $q = p^\alpha$ be a prime power. Let F be a function field of genus g over the finite field $\mathbb{F}_{q^2}$. Denote $N(F)$ the number of rational places of F. We call F a ($\mathbb{F}_{q^2}$-)*maximal function field* if $N(F)$ attains the Hasse-Weil upper bound [93]. i.e.

$$N(F) = q^2 + 1 + 2g\sqrt{q^2} = q^2 + 1 + 2gq.$$

The most important example of a maximal function field is the Hermitian function field $\mathcal{H}$, which is defined by $\mathcal{H} = \mathbb{F}_{q^2}(x, y)$, where x, y satisfies the equation

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

It has genus $\frac{1}{2}q(q-1)$. It can be shown that the Hermitian function field has the largest possible genus that a maximal function field can have, and it is the unique maximal function field having that genus. It can be shown that if a function field F is a subfield of a maximal function field E over the same constant field, then F is also maximal. Most of the known maximal function fields are subfields of $\mathcal{H}$, and therefore it is interesting to find maximal function fields that are not a subfield of $\mathcal{H}$.

Given a maximal function field $\mathcal{X}$, we want to check if $\mathcal{X}$ is a subfield of $\mathcal{H}$. If an extension $\mathcal{H}/\mathcal{X}$ exists,

from the general genus and splitting consideration, one can obtain some bounds on the degree $d = [\mathcal{H} : \mathcal{X}]$. In the case that $\mathcal{H}/\mathcal{X}$ is a Galois extension, we are able to say more. In the first part of the thesis, we obtain a new lower bound for the possible degrees. The idea is to analyze the Artin representation of $\mathcal{A} = \mathrm{Aut}(\mathcal{H}) = \mathrm{PGU}(3, q)$, and find out all the possible contributions of $\sigma \in \mathcal{A}$ to the ramification divisor of the extension $\mathcal{H}/\mathcal{X}$. It turns out that such a contribution is either very small or is very large, no contributions in the middle are possible. This reduces the problem of finding possible degrees of a covering to a problem of integer programming. The new lower bound of the degree is then obtained by solving the integer programming problem.

Having the lower bound in hand, we apply it to the generalized Giulietti-Korchmáros function fields (generalized GK function fields, in short). They are defined by $\mathcal{C}_n = \mathbb{F}_{q^{2n}}(x, y, z)$, with

$$x^q + x = y^{q+1},$$
$$y^{q^2} - y = z^{\frac{q^n+1}{q+1}},$$

for $q \geq 3$ and odd $n \geq 3$. As a result, we show that these function fields are not a Galois subfield of the Hermitian function field. For the family of function fields defined by the second equation above, i.e. $\mathcal{X}_n = \mathbb{F}_{q^{2n}}(y, z)$ with

$$y^{q^2} - y = z^{\frac{q^n+1}{q+1}},$$

we calculated concretely the range of possible degrees of a Galois extension from $\mathcal{X}_3$ to the Hermitian over the same field if it exists. In particular, for $n = 3$, we show that $\mathcal{X}_3$ is not a Galois subfield of the Hermitian function field when q is an odd prime by some additional group theoretic arguments.

1.2 Towers of function fields

It is well known that the Weil bound is not optimal when the genus g of a function field is large compared with the number of elements q in its constant field. The Ihara constant is a measure of the asymptotic behaviour of the number of rational places on function fields over a fixed finite field $\mathbb{F}_q$ when the genus becomes large. The Ihara constant is defined by

$$A(q) := \limsup_{g \to \infty} \frac{N_g(q)}{g},$$

where

$$N_q(g) := \max N(F),$$

with the maximum being taken over all function fields $F/\mathbb{F}_q$ with genus g. For any q, Drinfel′d and Vlăduţ [15] show that $A(q) \leq \sqrt{q} - 1$, and if q is a square, Ihara [46] and Tsfasman-Vlăduţ-Zink [86] show that $A(q) = \sqrt{q} - 1$. For a general q we know much less. Serre proved that $A(q) \geq c \log q$ for some absolute constant c by constructing infinite unramified class field towers over hyperelliptic curves.

The idea of Serre's class field tower method goes as follows. Suppose we have a curve X over $\mathbb{F}_q$, and let K be its corresponding function field, called the *ground field*. Let ℓ be a prime and S be a set of places in K. The (ℓ, S)-class field tower is unramified over K, and the places in S split completely. If the tower is finite, then its Galois group G is a finite ℓ-group. Let $d_\ell(G)$ and $r_\ell(G)$ be the generator rank and relation rank of G respectively. The Golod-Shafarevich inequality for a finite ℓ-group gives a relation between $d_\ell(G)$ and $r_\ell(G)$:

$$r_\ell(G) > \frac{d_\ell(G)^2}{4}.$$

Combining this with some estimates of $d_\ell(G)$ and the difference $r_\ell(G) - d_\ell(G)$, we may obtain a contradiction with these inequalities. That implies the Galois group G is infinite, and hence the tower is infinite. In this case, the asymptotic limit of the class field tower is a lower bound for $A(q)$.

There are many variants of Serre's class field tower method. One of them is given by Kuhnt in his PhD thesis [49]. His idea is to consider K as an extension of some suitably chosen k, and then consider the Galois group $\mathrm{Gal}(L/k)$ instead of $\mathrm{Gal}(L/K)$. He obtained inequalities for the generator rank and the relation rank of $\mathrm{Gal}(L/k)$, and successfully gets a good lower bound for $A(2)$. In particular, he gets $A(2) \geq 0.302325\ldots$.

In the second part of the thesis, we refine Kuhnt's idea and improve the lower bounds for $A(2)$ and $A(3)$ further. Given any function field k which we call the *base field*, and two disjoint sets S and T of places of k, we construct the class field tower in two steps: first we construct the l-ray class field K with controlled ramifications for the places in S, and such that all places of T split. The unramified class field tower L with splitting set T is then built on K. In this way we eliminate the need of an estimation of the generator rank of the class group of K, for which no sharp bounds are known in general. We determine conditions such that our construction yields infinite towers. This enables us to construct many class field towers, and for $q = 2, 3$ we are able to demonstrate new towers that are good enough to improve the previous known lower bounds on $A(q)$. Our results are the following.

Theorem 1.1. *Let $A(q)$ be the Ihara constant, then*

$$A(2) \geq 0.316999\ldots,$$
$$A(3) \geq 0.492876\ldots.$$

1.3 Selmer groups of elliptic curves over function fields

In the last part of the thesis, we change topic and study elliptic curves over function fields. More precisely, we study the Selmer groups arising from the 2-isogeny

$$\phi(x,y) = \left(\frac{y^2}{x^2}, \frac{y(abn^2 - x^2)}{x^2}\right)$$

for the family of elliptic curves with full 2-torsions,

$$E_n : \qquad y^2 = x(x+an)(x+bn)$$

over $K = \mathbb{F}_q(t)$, when q is odd. We show that the orders of the Selmer groups are almost always bounded by some constant independent of n. This is the function field analogue of Theorem 1 in [96]. Our strategy is to develop a function field analogue of the idea of Heath-Brown [41, 42] on the Selmer group problem over number fields. In particular, we bound the average order of the Selmer groups using character sums, and provide analogous estimates of these character sums in the function field case. The distribution of the Selmer groups then follows from a long and careful calculation.

1.4 Outline of the thesis

We begin with a brief revision on the basics of function fields in Chapter 2. Chapter 3-4 is the first part of our paper, in which we study maximal function fields. We define maximal function fields and study their basic properties in Chapter 3, and present our results about Galois subfields of the Hermitian function field in Chapter 4. The second part consists of Chapter 5-9. In Chapter 5, we define the generator rank and the relation rank. We then state the Golod-Shafarevich inequality, which is one of the central tools we will use in the study of class field towers. Chapter 6 reviews some basic class field theory that is vital in our tower construction. In Chapter 7 we define the embedding problem, which is the backbone of the induction steps of our towers. We then give a historic outline of the developments on the bounds for the Ihara constant, and outline Serre's class field tower method in Chapter 8, before we build our own towers in Chapter 9. In the last part of this thesis, we give the necessary backgrounds about elliptic curves over function fields and their Selmer groups in Chapter 10. The distribution of the ϕ-Selmer groups of E_n is then calculated in Chapter 11.

We remark that our results in Chapter 4 (except Theorem 4.2) is available in [17], and those in Chapter 9 are available in [16]. The last part about elliptic curves and their Selmer groups is an ongoing project,

and we hope that the first preprint will be available soon. In addition, some ideas for further research are discussed at the end of each part.

Chapter 2

Basics of function fields

In this chapter, we will outline some facts about function fields that will be useful in later chapters. The primary references for this chapter are [69, 80].

2.1 Function fields

Let k be a field. A *function field in one variable over* k is a field F containing k and at least one element x, transcendental over k, so that $F/k(x)$ is a finite algebraic extension. Equivalently, F has transcendence degree one over k. When $k = \mathbb{F}_q$ is a finite field, F is called a *congruence function field*. In this thesis we will restrict ourselves to congruence function fields, and so we refer them simply as *function fields* thereafter. When k is algebraically closed in F, the field k is called the *constant field* of F.

Example 2.1. The simplest example of a function field is the rational function field $k(x)$. Each element $z \in F^*$ can be represented uniquely as

$$z = a \prod_i p_i(x)^{n_i}$$

in which $a \in k^*$, $p_i \in K[x]$ are monic, pairwise distinct and irreducible, and n_i are nonzero integers.

A *place*, or a *prime*, in F is a discrete valuation ring R in F with maximal ideal P such that $k \subseteq R$. By abuse of notation, we say the maximal ideal P is a place in F. For a place P, we denote the corresponding normalized valuation function by v_P. Thus we have

$$\mathcal{O}_P := R = \{a \in F : v_P(a) \geq 0\},$$
$$P = \{a \in F : v_P(a) > 0\}.$$

The *degree* of P is by definition the degree of the residue field $\kappa(P) := \mathcal{O}_P/P$ over k, i.e.

$$\deg P = [\kappa(P) : k].$$

One can show that the degree is finite. We often denote the set of all places in F by $\mathbb{P}_F$. A place of degree one is also referred to as a *rational place*. This is the primary object of interest in the thesis. By a *local uniformizer* at P, we mean an element $\pi \in F$ such that $v_P(\pi) = 1$.

More generally, let T be a finite set of places in F. Define the *ring of T-integers* of F by

$$\mathcal{O}_T = \{z \in F : v_P(z) \geq 0 \ \forall P \in T\}.$$

We have $\mathcal{O}_T = \cap_{P \in T} \mathcal{O}_P$.

Example 2.2. Consider $F = k(x)$. To each irreducible polynomial $P(x) \in k[x]$ of degree d corresponds a place P of degree $\deg P = d$. There is only one more place in F. Consider the valuation map $v_\infty : F \to \mathbb{Z}$ defined by $v_\infty(f/g) = \deg g - \deg f$. The corresponding place for this valuation is denoted P_∞, called the *place at infinity*. It is also called the pole of x since $v_\infty(x) = -1$. This place has degree one.

Next we look at extensions of function fields. Let E/F be an extension of function fields, and let k be the constant field of F. Let l be the algebraic closure of k in E. It is clear that l is the constant field of E. If $E = lF$ we say that E is a *constant field extension* of F, and if $k = l$ we say that E is a *geometric extension* of F.

Let E/F be an extension of function fields, and let $\mathfrak{P}, P$ be places in E, F respectively. We say that $\mathfrak{P}$ lies above P if $P = \mathfrak{P} \cap F$, and we write $\mathfrak{P}|P$. Every place $\mathfrak{P}$ of E lies above a place P of F, and every place P of E lies under some place $\mathfrak{P}$ of F. To each pair $\mathfrak{P}|P$ we associate two integers. The *relative degree* $f = f(\mathfrak{P}|P)$ is the degree of the residue field extension $[\mathcal{O}_\mathfrak{P}/\mathfrak{P} : \mathcal{O}_P/P]$, and the *ramification index* $e = e(\mathfrak{P}|P)$ is the integer such that $v_\mathfrak{P}(a) = e \cdot v_P(a)$ for all $a \in F$. The numbers e and f behave multiplicatively in towers. In a finite, separable extension, the e and f are governed by the following fundamental equality [69, Prop. 7.2].

Theorem 2.3. *Let E/F be a finite, separable extension of function fields, and $P\mathcal{O}_E = \mathfrak{P}_1^{e_1} \dots \mathfrak{P}_g^{e_g}$ the decomposition of the place P in E. Let $e_i = e(\mathfrak{P}_i|P)$ and $f_i = f(\mathfrak{P}_i|P)$. We have*

$$\sum_{i=1}^{g} e_i f_i = n = [E : F].$$

Moreover, if the extension E/F is Galois, then all the e_i's and all the f_i's are equal, and we have $efg = n$.

Let E/F be an extension of function fields with characteristic p and let $\mathfrak{P}, P$ be places in E, F respectively. If $\mathfrak{P}$ is a place above P, we say that $\mathfrak{P}|P$ is ramified if $e = e(\mathfrak{P}|P) > 1$, and is unramified otherwise. If $\mathfrak{P}|P$ is ramified, we say that the ramification is *wild* if $p|e$, and is *tame* otherwise. The extension E/F is

said to be *unramified* if no places in F ramify in E, is *tame* if no places in F are wildly ramified, and is *wild* otherwise.

We will close this section by the following remark relating function fields with curves.

Remark 2.4. The theory of function fields can also be stated in terms of curves over finite fields thanks to the function field and curve correspondence, which says that there is an arrow-reversing equivalence of categories between the nonsingular curves with nonconstant morphisms and the function fields with inclusions. Here, by a *curve* we mean a nonsingular, projective, irreducible curve over some field k. In the language of curves, a rational place corresponds to a rational point on the curve, and an extension of function fields corresponds to a covering of curves. In this thesis, we will stick with the notation of function fields except for the last two chapters, where we will talk about elliptic curves over function fields.

Example 2.5. The curve corresponding to the function field $F = k(x)$ is the projective line $\mathbb{P}^1(k)$. Each finite rational place of F comes from an irreducible polynomial $x - a$ for some $a \in k$. This corresponds to the point $[a : 1]$ in $\mathbb{P}^1(k)$. The infinite place P_∞ corresponds to the point at infinity $[1 : 0]$.

2.2 Divisors, genus and the Hurwitz genus formula

The *group of divisors* of F, $\mathrm{Div}(F)$, is the free abelian group generated by the places in F. Thus a divisor can be written in the form

$$D = \sum_{P \in \mathbb{P}_F} v_P(D)P, \tag{2.1}$$

where $v_P(D) \in \mathbb{Z}$ and all but finitely many $v_P(D)$ are zero. The *support* of D, $\mathrm{Supp}(D)$, is the set of all P such that $v_P(D) \neq 0$. The degree of a divisor as in (2.1) is $\deg D = \sum_P v_P(D) \deg P$. This definition induces a map $\deg : \mathrm{Div}(F) \to \mathbb{Z}$, whose kernel we denote by $\mathrm{Div}^0(F)$.

We can describe some elements in $\mathrm{Div}^0(F)$ explicitly. For an element $a \in F^*$, define the divisor

$$(a) := \sum_P v_P(a)P.$$

It can be shown that (a) has degree zero for any $a \in F^*$ [69, Prop. 5.1]. These divisors are called the *principal divisors*. Let $\mathcal{P}(F)$ be the set of all principal divisors in F. We define

$$Cl(F) = \mathrm{Div}(F)/\mathcal{P}(F),$$
$$Cl^0(F) = \mathrm{Div}^0(F)/\mathcal{P}(F).$$

More generally, let T be a finite non-empty set of places of F. The *group of T-divisors*, $\mathrm{Div}_T(F)$, is the subgroup of $\mathrm{Div}(F)$ consisting of divisors whose supports are disjoint from T. Given any element $a \in K^*$, we define its *T-divisor* to be

$$(a)_T = \sum_{P \notin T} v_P(a)P.$$

The principal T-divisors form a subgroup $\mathcal{P}_T(F)$, and the quotient

$$Cl_T(F) = \mathrm{Div}_T(F)/\mathcal{P}_T(F)$$

is called the *T-class group* of F. Let $D = \sum_P v_P(D)P$ be a divisor whose support is disjoint from T, and define the set

$$\mathcal{P}_T^D(F) = \{(a) \in \mathcal{P}_T(F) : a \in \mathcal{O}_T \text{ and } v_P(a-1) \geq v_P(D)\ \forall P \in \mathrm{Supp}(D)\}.$$

The *T-ray class group* with modulus D is then the quotient $Cl_T^D(F) = \mathrm{Div}_T(F)/\mathcal{P}_T^D(F)$.

A divisor D as in (2.1) is *effective* if $v_P(D) \geq 0$ for all P. Two divisors D_1 and D_2 are *linearly equivalent*, denoted by $D_1 \sim D_2$, if $D_1 - D_2 \in \mathcal{P}_F$ is principal. Define

$$L(D) = \{x \in F^* : (x) + D \geq 0\} \cup \{0\}. \tag{2.2}$$

This is a finite dimensional vector space, and if $\deg(D) \leq 0$, then $L(D) = \{0\}$ unless $D \sim 0$, in which case $L(D) \cong k$. Denote by $\ell(D)$ the dimension of $L(D)$. An important result of the $\ell(D)$ is the Riemann-Roch theorem.

Theorem 2.6 (Riemann-Roch)**.** *There is an integer $g \geq 0$ and a divisor class $\mathcal{C}$ such that for $C \in \mathcal{C}$ and $D \in Div(F)$, we have*

$$\ell(D) - \ell(C - D) = \deg(D) - g + 1.$$

Proof. See [69, Chap. 6] or [80, §1.5]. □

The integer g in the above theorem is an important invariant of F called the *genus*, and $\mathcal{C}$ is called the *canonical class* of F. Any divisor $C \in \mathcal{C}$ is called a *canonical divisor*. Two useful corollaries of the Riemann-Roch are the following.

Corollary 2.7. *1. For a canonical divisor C, $\deg(C) = 2g - 2$ and $\ell(C) = g$.*

2. If $\deg(D) \geq 2g - 2$, then $\ell(D) = \deg(D) - g + 1$ except when $D \in \mathcal{C}$, for which $\deg(D)$ and $\ell(D)$ are

given by the above part.

Remark 2.8. In the language of curves, let X be a curve and $\mathcal{O}_X$ be its structure sheaf. One can define the genus g of a curve X to be the k-dimension of the cohomology group $H^1(X, \mathcal{O}_X)$. Topologically, one can view X as a Riemann surface, and g is the "number of holes" of X. See [40, Chap. 4] for more details.

Next we look at the behaviour of the genus under field extensions. Recall our assumption that all the function fields we are considering have finite constant fields. The first two results show that the genus is unchanged under purely inseparable extensions and constant field extensions.

Proposition 2.9 (Prop. 7.5 of [69]). *If F has perfect constant field, and if E/F is a finite extension, then $g(E) = g(F)$.*

Proposition 2.10 (Prop 8.9 of [69]). *Suppose F has perfect constant field k and l/k is a finite extension. Let $E = lF$. We have $g(E) = g(F)$.*

Having the above propositions in hand, we can restrict our attention to separable geometric extensions. Let E/F be one such extension, with k, l the constant fields of F, E respectively. Let P be a place in F and $\mathcal{O}_P$ its local ring. Let $\mathcal{O}'_P$ be the integral closure of $\mathcal{O}_P$ in E. Let $\mathrm{Tr}_{E/F}$ be the trace map. Define the *complementary module* by

$$\mathcal{C}_P = \{z \in E : \mathrm{Tr}_{E/F}(z\mathcal{O}'_P) \subseteq \mathcal{O}_P\}.$$

It can be shown that $\mathcal{C}_P = \mathcal{O}'_P$ for all but finitely many P. For each P, there is an element $t \in E$ (depending on P) such that $\mathcal{C}_P = t\mathcal{O}'_P$, and $v_{\mathfrak{P}}(t) \leq 0$ for all $\mathfrak{P}|P$. Moreover, such t is unique in the sense that if $\mathcal{C}_P = t'\mathcal{O}'_P$, then $v_{\mathfrak{P}}(t) = v_{\mathfrak{P}}(t')$ for all $\mathfrak{P}|P$ (see [80, §3.4]). Therefore, it make sense to define the *different exponent* of $\mathfrak{P}$ over P by

$$d(\mathfrak{P}|P) := -v_{\mathfrak{P}}(t). \tag{2.3}$$

Define the *different* (or the different divisor) of E/F to be the divisor

$$\mathrm{Diff}(E/F) := \sum_P \sum_{\mathfrak{P}|P} d(\mathfrak{P}|P)\mathfrak{P}.$$

This is well-defined since $\mathcal{C}_P = \mathcal{O}'_P$ for almost all P, and is effective by (2.3). The different exponent and the ramification index are related by Dedekind's different theorem [80, Theorem 3.5.1].

Proposition 2.11 (Dedekind's different theorem). *Settings as above. For all $\mathfrak{P}|P$, we have*

1. $d(\mathfrak{P}|P) \geq e(\mathfrak{P}|P) - 1$,

2. $d(\mathfrak{P}|P) = e(\mathfrak{P}|P) - 1$ *if and only if the ramification of* $\mathfrak{P}|P$ *is tame.*

In particular, we see that $\mathfrak{P}|P$ is unramified if and only if $d(\mathfrak{P}|P) = 0$. We are now ready to state an important theorem that relates $g(E)$ and $g(F)$.

Theorem 2.12 (Hurwitz's genus formula)**.** *Let E/F be a finite separable extension of function fields, and let l, k be the constant fields of E, F respectively. We have*

$$2g(E) - 2 = \frac{[E:F]}{[l:k]}(2g(F) - 2) + \deg \mathrm{Diff}(E/F).$$

Proof. See [69, Chap. 7] or [80, §3.4]. □

If E/F is Galois, we can express the different exponent $d(\mathfrak{P}|P)$ in another way by the Hilbert different formula (see the proof in [80, Theorem 3.8.7]). Let $G = \mathrm{Gal}(E/F)$, and let $\mathfrak{P}$ be a place in E above P in F. The different exponent $d(\mathfrak{P}|P)$ is

$$d(\mathfrak{P}|P) = \sum_{\substack{1 \neq \sigma \in G \\ \sigma(\mathfrak{P}) = \mathfrak{P}}} i_{\mathfrak{P}}(\sigma), \tag{2.4}$$

where $i_{\mathfrak{P}}(\sigma) = v_{\mathfrak{P}}(\sigma(t) - t)$ with t a local uniformizer at $\mathfrak{P}$. Note that if the ramification of $\mathfrak{P}$ over P is tame, then $i_{\mathfrak{P}}(\sigma) = 1$ for any σ that fixes $\mathfrak{P}$, and in that case $d(\mathfrak{P}|P)$ is the number of elements $\sigma \neq 1$ in G that fix $\mathfrak{P}$.

For any $\sigma \in G$, define

$$i(\sigma) := \sum_{\mathfrak{P} \in \mathbb{P}_E} i_{\mathfrak{P}}(\sigma) \deg \mathfrak{P}, \tag{2.5}$$

with the convention that $i_{\mathfrak{P}}(\sigma) = 0$ if $\sigma(\mathfrak{P}) \neq \mathfrak{P}$. Combining (2.4) with the Hurwitz genus formula, we get the following theorem.

Theorem 2.13. *Suppose E/F is a geometric Galois field extension of degree d with Galois group G, then*

$$2g(E) - 2 = d(2g(F) - 2) + \deg R,$$

where R is the ramification divisor, whose degree is given by

$$\deg R = \sum_{1 \neq \sigma \in G} i(\sigma),$$

with $i(\sigma)$ defined as in (2.5).

Finally, we end this section with some properties of $i(\sigma)$ that will be useful later.

Proposition 2.14. *In the above notations, we have*

1. *$i(\sigma)$ only depends on the conjugate class of σ. i.e. for any $\sigma, \tau \in G$, $i(\tau\sigma\tau^{-1}) = i(\sigma)$.*

2. *If Q is a group of prime order p, then $i(\sigma)$ is the same for every nontrivial element $\sigma \in Q$.*

Proof. We will prove both parts at the level of $i_{\mathfrak{P}}(\sigma)$. A fancy proof of part 1 can be obtained by noting that $i(\sigma)$ is the negative of the Artin character, see Section 4.3 for more details. Alternatively, let t be a local uniformizer at $\mathfrak{P}$, we can calculate

$$\begin{aligned} i(\tau\sigma\tau^{-1}) &= v_{\mathfrak{P}}(\tau\sigma\tau^{-1}t - t) \\ &= v_{\mathfrak{P}}(\tau\sigma\tau^{-1}t - \tau\tau^{-1}t) \\ &= v_{\mathfrak{P}}(\tau(\sigma\tau^{-1}t - \tau^{-1}t)) \\ &= v_{\mathfrak{P}}(\sigma(\tau^{-1}t) - \tau^{-1}t) \\ &= i(\sigma). \end{aligned}$$

Here in the third equality we use the fact that an automorphism τ preserves valuation, and in the last step we use the fact that $i_{\mathfrak{P}}(\sigma)$ is independent of the choice of a uniformizer.

For part 2, let σ be a nontrivial element in Q, so that $Q = \{\sigma^k | 0 \leq k \leq p-1\}$. Let $\mathfrak{P} \in \mathbb{P}_E$. If σ does not fix $\mathfrak{P}$, then every nontrivial element in Q will not fix $\mathfrak{P}$. So $i(\sigma^k) = 0$ for any $1 \leq k \leq p-1$. If σ fixes $\mathfrak{P}$, then every element in Q will fix $\mathfrak{P}$. Again let t be a local uniformizer at $\mathfrak{P}$, we have

$$\begin{aligned} i_{\mathfrak{P}}(\sigma^k) = v_{\mathfrak{P}}(\sigma^k t - t) &= v_{\mathfrak{P}}((\sigma(\sigma^{k-1}t) - \sigma^{k-1}t) + (\sigma^{k-1}t - t)) \\ &\geq \min\{v_{\mathfrak{P}}(\sigma(\sigma^{k-1}t) - \sigma^{k-1}t), v_{\mathfrak{P}}(\sigma^{k-1}t - t)\} \\ &= \min\{v_{\mathfrak{P}}(\sigma u - u), i_{\mathfrak{P}}(\sigma^{k-1})\} \\ &= \min\{i_{\mathfrak{P}}(\sigma), i_{\mathfrak{P}}(\sigma^{k-1})\} \\ &\geq \min\{i_{\mathfrak{P}}(\sigma), i_{\mathfrak{P}}(\sigma), i_{\mathfrak{P}}(\sigma^{k-2})\} \\ &\geq \dots \\ &\geq i_{\mathfrak{P}}(\sigma). \end{aligned}$$

In the third line we used the fact that $u = \sigma^{k-1}(t)$ is also a local uniformizer at $\mathfrak{P}$ as σ is an automorphism. Now as the above calculation is true for any nontrivial element in Q, we conclude that all $i_{\mathfrak{P}}(\sigma^k)$, for $1 \leq k \leq p-1$, are equal. □

Later we will need another variant of the Hurwitz genus formula for abelian extensions, obtained by class field theory. The formula will be stated in Theorem 6.7.

2.3 Zeta function and L-polynomial

Let q be a prime power and F be a function field with constant field $k = \mathbb{F}_q$. In this section, we will define the zeta function of F and more generally L-series attached to F, and investigate some of their properties.

Let $D \in \mathrm{Div}(F)$ be an effective divisor. We define the norm of D, denoted ND, to be $q^{\deg(D)}$. Note that if D_1, D_2 are two effective divisors, then $\mathcal{N}(D_1 + D_2) = (\mathcal{N}D_1)(\mathcal{N}D_2)$. We are now able to define the *zeta function* of F.

Definition 2.15. The zeta function of F is defined by

$$\zeta_F(s) = \sum_{D \geq 0} \frac{1}{\mathcal{N}D^s}.$$

Here the sum runs through all effective divisors $D \in \mathrm{Div}(F)$.

We remark that if the underlying function field F is clear, we may write $\zeta(s)$ and omit the function field F.

Example 2.16. Let $F = \mathbb{F}_q(x)$ and $R = \mathbb{F}_q[x]$. It is easy to see that for $\mathrm{Re}(s) > 1$, one can express $\zeta_F(s)$ as an Euler product

$$\zeta_F(s) = \prod_P \left(1 - \frac{1}{\mathcal{N}P^s}\right)^{-1}.$$

The place at infinity P_∞ contributes $(1 - q^{-s})$ to the above product, and the product over all finite places is equal to the sum

$$\zeta_R(s) = \sum_{f \in A \text{ monic}} \frac{1}{|f|^s},$$

where $|f| = q^{\deg f}$. In the ring R, there are exactly q^n monic polynomials of degree n. Thus

$$\zeta_R(s) = \sum_{n=0}^{\infty} \frac{q^n}{q^{ns}} = \frac{1}{1 - q^{1-s}}$$

and hence

$$\zeta_F(s) = \frac{1}{(1 - q^{-s})(1 - q^{1-s})}.$$

Note that $\zeta_F(s)$ is, a priori, defined only for $\mathrm{Re}(s) > 1$, but the right hand side of the above formula gives an analytic continuation of $\zeta_F(s)$ to all of $\mathbb{C}$ except for isolated simple poles.

In general, the zeta function of F is a rational function in $T = q^{-s}$. More precisely, we have the following.

Theorem 2.17. *Let $F/\mathbb{F}_q$ be a function field with genus g. Then there exists some polynomial $L_F(u) \in \mathbb{Z}[u]$ of degree $2g$ such that*

$$\zeta_F(s) = \frac{L_F(q^{-s})}{(1-q^{-s})(1-q^{1-s})}$$

for $Re(s) > 1$. The right hand side of the above formula gives an analytic continuation of $\zeta_F(s)$ to all of $\mathbb{C}$ except for isolated simple poles.

The polynomial $L_F(u)$ in the above theorem is called the *L-polynomial* of F. Again when the underlying function field F is clear, we may omit it from the notation and write $L(u)$. The L-polynomial contains a lot of information about the function field F. Some of them are listed below.

Theorem 2.18. *The L-polynomial $L(u)$ of a function field $F/\mathbb{F}_q$ satisfies the following:*

1. *(Functional equation) $L(u) = q^g u^{2g} L(1/qu)$.*
2. *$L(1) = h$ is the class number of F.*
3. *Write $L(u) = a_0 + a_1 u + \ldots + a_{2g} u^{2g}$, then the coefficients a_j satisfy*
   (a) *$a_0 = 1$ and $a_{2g} = q^g$,*
   (b) *$a_{2g-j} = q^{g-j} a_j$ for $0 \le j \le g$,*
   (c) *$a_1 = N(F) - (q+1)$, where $N(F)$ is the number of rational places of F.*
4. *(Riemann Hypothesis) Factor $L(u)$ into a product of linear complex polynomials*

$$L(u) = \prod_{j=1}^{2g} (1 - \alpha_j u).$$

   Then the reciprocal roots α_j are algebraic integers satisfying $|\alpha_j| = q^{1/2}$ for all $1 \le j \le 2g$.

5. *Again write*

$$L_F(u) = \prod_{j=1}^{2g} (1 - \alpha_j u).$$

   If $F_r = \mathbb{F}_{q^r} F$ is the constant field extension of degree r over F, then

$$L_{F_r}(u) = \prod_{j=1}^{2g} (1 - \alpha_j^r u).$$

Proof. See [80, Chap. 5]. For the Riemann hypothesis, Weil's original treatments can be found in [93, 94]. For other treatments, see Bombieri [7] and Stöhr-Voloch [82]. □

By (3c) of the above theorem, we can write $\alpha_j = \sqrt{q}e^{i\theta_j}$, with $-\pi \leq \theta_j < \pi$. The θ_j are called the *Frobenius angles* of F. One immediate consequence of (3c) and (4) of the above theorem is the celebrated Weil bound on the number of rational places of F. We will return to this subject in Chapter 3. The last proposition of this section shows how the L-polynomial behaves under field extensions.

Proposition 2.19. *Let E/F be a geometric extension of function fields. Then L_F divides L_E.*

Proof. See [69, Chap. 9]. □

2.4 Average values in function fields

Recall that $\mathrm{Div}(F)$ is the group of divisors of F. Let $\mathrm{Div}^+(F)$ be the semigroup of effective divisors of F including the zero divisor. An *arithmetic function* on F is a function $f : \mathrm{Div}^+(F) \to \mathbb{C}$. It is *multiplicative* if for all $D_1, D_2 \in \mathrm{Div}^+(F)$, we have $f(D_1 + D_2) = f(D_1)f(D_2)$. The *Dirichlet series* associated to f is defined by

$$\zeta_f(s) = \sum_{D \in \mathrm{Div}^+(F)} \frac{f(D)}{\mathcal{N}D^s}. \tag{2.6}$$

Let $F(N) = \sum_{\deg D = N} f(D)$, then (2.6) can be rewritten as

$$\zeta_f(s) = \sum_{N=0}^{\infty} F(N) q^{-Ns}.$$

Example 2.20. Consider $f(D) = 1$ for all D. Then $\zeta_f(s)$ is the zeta function $\zeta_F(s)$ of F. The function $F(N) = \sum_{\deg D = N} f(D)$ counts the number of effective divisor of degree N. When $N = 0$, $F(N) = 1$, and when $N = 1$, $F(1)$ is the number of rational places $N(F)$ of F. For $N > 2g - 2$, Riemann-Roch (Theorem 2.6) tells us that

$$F(N) = h \cdot \frac{q^{N+1-g} - 1}{q - 1},$$

where h is the class number of F.

In this thesis, we are interested in estimating $F(N)$ for various arithmetic function f, in particular when $N \to \infty$. A useful theorem in this direction is the Wiener-Ikehara Tauberian theorem, which relates the estimation of $F(N)$ to the analyticity of $\zeta_f(s)$ in a certain region.

Theorem 2.21 (Tauberian theorem; Theorem 17.1 of [69]). *Let f be an arithmetic function on F. Define the region*

$$B = \{s \in \mathbb{C} : \frac{-\pi i}{\log q} \leq \mathrm{Im}(s) < \frac{\pi i}{\log q}\}.$$

Suppose that $\zeta_f(s)$ converges absolutely for $\mathrm{Re}(s) > 1$, and is holomorphic on the part of the vertical line $\mathrm{Re}(s) = 1$ inside B, except possibly for a simple pole at $s = 1$ with residue α. Then there is a $\delta < 1$ such that

$$\sum_{\deg D = N} f(D) = \alpha q^N \log q + O(q^{\delta N}).$$

Furthermore, if $\zeta_f(s)$ is holomorphic in $B \cap \mathrm{Re}(s) \geq \delta'$ except only at $s = 1$, then the error term in the above estimate can be replaced by $O(q^{\delta' N})$.

We will end this section with the following lemma, which is the function field analogue of [37, Theorem 01]. It will be useful in Chapter 11 where there are some functions f such that Theorem 2.21 does not apply.

Lemma 2.22. *Let f be a non-negative multiplicative function on $K = \mathbb{F}_q(t)$. Suppose there exists constants A and B such that the following two conditions are satisfied:*

1. $\sum_{\substack{\deg P = N \\ P \text{ prime}}} f(P) \deg P \leq Aq^N$ *(i.e.* $\sum_{\substack{\deg P = N \\ P \text{ prime}}} f(P) \leq A\frac{q^N}{N}$*),*
2. $\sum_{P \text{ prime}} \sum_{v \geq 2} \frac{f(P^v)}{|P|^v} \deg(P^v) \leq B.$

Then for $N \geq 1$, we have

$$\sum_{\deg n = N} f(n) \leq (A + B)\frac{q^N}{N} \sum_{\deg n = N} \frac{f(n)}{|n|}.$$

Here the sum is over all monic polynomials $n \in K$ of degree N.

Proof. We will follow the idea in [37]. First we claim that

$$N \sum_{\deg n = N} f(n) \leq \sum_{\substack{v, P \\ v \deg P \leq n}} f(P^v) \deg(P^v) \sum_{\deg m = N - v \deg P} f(m). \tag{2.7}$$

To see this, note that for any monic n with degree N, $f(n)$ appears with multiplicity exactly N in the left-hand-side of (2.7). Write $n = P_1^{k_1} \dots P_r^{k_r}$ as the prime factorization of n. In the right-hand-side, $f(n)$ appears with multiplicity $\deg(P_i^{k_i})$ for every decomposition $n = P_i^{k_i} M$, and so the total multiplicity is $\sum_i \deg(P_i^{k_i}) = \deg n = N$. As all other mixed terms are non-negative, we get the desired formula.

Now write the right-hand-side of (2.7) into $S_1 + S_2$, where

$$S_1 = \sum_{\deg P \le n} f(P)\deg(P) \sum_{\deg m = N - \deg P} f(m),$$
$$S_2 = \sum_{\substack{v \ge 2, P \\ v \deg P \le n}} f(P^v)\deg(P^v) \sum_{\deg m = N - v\deg P} f(m).$$

Denote

$$S(N) = \sum_{\deg n \le N} \frac{f(n)}{|n|},$$

we have

$$\begin{aligned} S_1 &= \sum_{\deg P \le n} f(P)\deg(P) \sum_{\deg m = N - \deg P} f(m) \\ &\le \sum_{\deg m \le N} f(m) \sum_{\deg P = n - \deg M} f(P)\deg P \\ &\le \sum_{\deg m \le N} f(m)(Aq^{N - \deg m}) \\ &= Aq^N S(N), \end{aligned} \tag{2.8}$$

where in the penultimate step we used condition 1. For S_2, we have

$$\begin{aligned} S_2 &= \sum_{\substack{v \ge 2, P \\ v \deg P \le n}} f(P^v)\deg(P^v) \sum_{\deg m = N - v\deg P} f(m) \\ &= \sum_{\substack{v \ge 2, P \\ v \deg P \le n}} f(P^v)\deg(P^v) \sum_{\deg m = N - v\deg P} f(m) \left(\frac{q^N}{q^{v \deg P} q^{\deg m}} \right) \\ &= q^N \sum_{\substack{v \ge 2, P \\ v \deg P \le n}} \frac{f(P^v)\deg(P^v)}{|P|^v} \sum_{\deg m = N - v\deg P} \frac{f(m)}{|m|} \\ &\le Bq^N S(N). \end{aligned} \tag{2.9}$$

Here in the last step we used condition 2. Finally, substituting (2.8) and (2.9) into (2.7) completes the proof of the lemma. □

Chapter 3

Maximal function fields

In this chapter we give a brief overview of currently known bounds for the number of rational places of a function field F. After that, we will define maximal function fields and give some examples of such fields. Finally, we will give some properties of subfields of a maximal function field. The main references for this chapter are [66, 80]

3.1 Upper bounds for the number of rational places

In this section we give several bounds for the number of rational places of a function field F. Let q be a prime power, and let F be a function field with constant field $k = \mathbb{F}_q$, and let $N(F)$ be the number of rational places of F. The classical bound for $N(F)$ is the Weil bound.

Theorem 3.1 (Weil)**.** *If F is a function field over $\mathbb{F}_q$ with genus g, we have*

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

Proof. This follows directly from part (3c) and (4) of Theorem 2.18. More precisely, let

$$L(u) = a_0 + a_1 u + \ldots + a_{2g}u^{2g} = \prod_{i=1}^{2g}(1 - \alpha_i u).$$

Compare the coefficient of a_1 and by Theorem2.18(3c), we have

$$a_1 = N(F) - (q+1) = \sum_{i=1}^{2g} \alpha_i.$$

The Weil bound now follows from the Riemann Hypothesis over function fields. □

The Weil bound can be attained when q is a square (see the next section), but one can improve it in an obvious way by noting that $N(F)$ is an integer, thus $|N(F) - (q+1)| \leq [2g\sqrt{q}]$, where $[\cdot]$ is the floor

function. Serre, however, improves the bound in a non-trivial way.

Theorem 3.2 (Serre)**.** *If F is a function field over $\mathbb{F}_q$ with genus g, we have*

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

Proof. See [80, Theorem 5.3.1]. □

On the other hand, if we fix the constant field $\mathbb{F}_q$ and let g increase, then the Weil bound become weak. In particular, the Weil bound cannot be attained when the genus goes beyond a certain limit. This is the scope of the next theorem.

Theorem 3.3 (Ihara)**.** *If F is a function field over $\mathbb{F}_q$ with genus g, and suppose that F attains the Weil upper bound, i.e.*

$$N(F) = q + 1 + 2g\sqrt{q},$$

then $g \leq \sqrt{q}(\sqrt{q}-1)/2$.

Ihara's theorem is the best possible: for any square q, there exists function field $F/\mathbb{F}_q$ of genus $g = \sqrt{q}(\sqrt{q}-1)/2$ such that $N(F)$ attains the Weil upper bound. In general, one can obtain upper bounds for $N(F)$ in terms of g by the Serre's explicit formula method.

Proposition 3.4 (Serre's explicit formula method)**.** *Let F be a function field over $\mathbb{F}_q$ with genus g, and let m be a positive integer. Define*

$$\lambda_m(t) = \sum_{i=1}^{m} c_r t^r$$

and $f_m(t) = 1 + \lambda_m(t) + \lambda_m(t^{-1})$. Suppose $c_1, \ldots, c_m \in \mathbb{R}$ satisfy the following:

1. *$c_r \geq 0$ for all i, and not all of them are zero.*
2. *$f_m(t) \geq 0$ for all $t \in \mathbb{C}$ with $|t| = 1$.*

Then

$$N(F) \leq \frac{g}{\lambda_m(q^{-1/2})} + \frac{\lambda_m(q^{1/2})}{\lambda_m(q^{-1/2})} + 1.$$

Proof. See [80, §5.3]. □

Example 3.5. As an example of the Serre's explicit formula, let $c_1 = 1/2$ and $c_r = 0$ for all $r > 1$. Then for $t = e^{i\theta}$,

$$f_m(t) = 1 + \frac{1}{2}t + \frac{1}{2}t^{-1} = 1 + \frac{1}{2}(e^{i\theta} + e^{-i\theta}) = 1 + \cos\theta \geq 0.$$

So by Proposition 3.4, we have

$$N(F) \leq \frac{g}{\frac{1}{2}q^{-1/2}} + \frac{\frac{1}{2}q^{1/2}}{\frac{1}{2}q^{-1/2}} + 1 = q + 1 + 2g\sqrt{q}.$$

This is the Weil bound. Next, let $c_1 = 2/3, c_2 = 1/3$ and $c_r = 0$ for all $r > 2$. Then for $t = e^{i\theta}$,

$$\begin{aligned} f_m(t) &= 1 + \frac{2}{3}t + \frac{2}{3}t^{-1} + \frac{1}{3}t^2 + \frac{1}{3}t^{-2} \\ &= 1 + \frac{2}{3}(e^{i\theta} + e^{-i\theta}) + \frac{1}{3}(e^{2i\theta} + e^{-2i\theta}) \\ &= 1 + \frac{4}{3}\cos\theta + \frac{4}{3}\cos^2\theta - \frac{2}{3} \\ &= \frac{1}{3}(1 + 2\cos\theta)^2 \geq 0. \end{aligned}$$

Thus we have the upper bound

$$N(F) \leq \frac{q^2 + 2q^{3/2} + 3gq}{2q^{1/2} + 1} + 1.$$

When g is large, this is better than the Weil bound since the coefficient of g is approximately $\frac{3}{2}\sqrt{q}$. We can push this type of argument further to obtain an "asymptotic upper bound" for $N(F)$ with respect to g, called the Drinfel′d-Vlăduţ bound. See 8.2 in Chapter 8.

3.2 Maximal function fields

In this section we define maximal function fields, and give some examples and basic properties of such fields.

Definition 3.6. Let m be a prime power, and let F be a function field over $\mathbb{F}_m$. We say that F is a *maximal function field* if the number of rational places on F, $N(F)$, attains the Weil upper bound. That is,

$$N(F) = m + 1 + 2g\sqrt{m}.$$

Notice that in order for a maximal function field to exist over $\mathbb{F}_m$, m has to be a square. To simplify our notations, we will write $m = q^2$ and assume that our function fields are over $\mathbb{F}_{q^2}$.

Tracing the proof of Theorem 3.1 and using Theorem 2.18 immediately reveals the following facts.

Proposition 3.7. *1. F is maximal if and only if all of its Frobenius angles are $-\pi$. Thus F is maximal if and only if the L-polynomial of F is $L(u) = (1 + qu)^{2g}$.*

2. If F is maximal, then $F_r = \mathbb{F}_{q^{2r}}F$ is maximal if and only if r is odd.

By Ihara's theorem (Theorem 3.3), the genus of any maximal function field $F/\mathbb{F}_{q^2}$ satisfies $g \leq q(q-1)/2$. This upper bound is attained by the Hermitian function field $\mathcal{H}$, defined by $\mathcal{H} = \mathbb{F}_{q^2}(x, y)$, with

$$y^q + y = x^{q+1}. \tag{3.1}$$

It is shown in [70] that the Hermitian function field is the unique maximal function field having genus $q(q-1)/2$.

It is not the case that for every genus $g < q(q-1)/2$ there exists a maximal function field of genus g. The second largest possible genus for a maximal function field is $g = (q-1)^2/4$ for q odd, and $g = [(q-1)^2/4] = q(q-2)/4$ for q even [21, 81]. Maximal function fields of these genera are known to exist. For odd q, a characterization of maximal function fields with genus $(q-1)^2/4$ is given by Fuhrmann, Garcia and Torres [20]. For even q, a partial characterization of maximal function fields with genus $q(q-2)/4$ is given by Abdón and Torres [2]. Determining the third largest genus that a maximal function field can have is an open problem.

3.3 Examples of maximal function fields

Three well-known maximal function fields over $\mathbb{F}_{q^2}$ are constructed via Deligne-Lusztig theory [14, 38, 39]. They are the Hermitian function field, the Suzuki function field and the Ree function field. Note that all of them can actually be defined over $\mathbb{F}_q$.

We have already encountered the Hermitian function field $\mathcal{H}$. It is defined by $\mathcal{H} = \mathbb{F}_{q^2}(x, y)$, with

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

Its genus is $g(\mathcal{H}) = q(q-1)/2$, which is the largest possible genus that a maximal function field can have. The number of rational places on $\mathcal{H}$ is $q^2+1+2qg(\mathcal{H}) = q^3+1$. Its automorphism group is $\mathrm{Aut}(\mathcal{H}) = PGU(3, q)$. There is another useful description of the Hermitian function field: Choose elements $a, b \in \mathbb{F}_{q^2}$ such that $a^q + a = b^{q+1} = -1$, and let

$$u = \frac{y+a}{x}, \qquad v = \frac{b(y+a+1)}{x}.$$

Then $\mathcal{H} = \mathbb{F}_{q^2}(u, v)$ with

$$u^{q+1} + v^{q+1} + 1 = 0. \tag{3.2}$$

Remark 3.8. In the language of projective geometry, the q^3+1 rational points on the Hermitian curves form

a *unital* in the projective plane, and $PGU(3,q)$ is the group that preserve this unital. See [43] for details.

When $q = 2q_0^2 > 2$, we have the Suzuki function field $\mathcal{S}$ over $\mathbb{F}_{q^2}$, defined by $\mathcal{S} = \mathbb{F}_{q^2}(x,y)$ with

$$y^q + y = x^{q_0}(x^q + x).$$

It has genus $q_0(q-1)$ and its automorphism group is isomorphic to the Suzuki group $Sz(q)$. The Suzuki function field is not maximal over $\mathbb{F}_{q^2}$, but it becomes maximal over $\mathbb{F}_{q^4}$.

Similar to the case of characteristic two, when $q = 3q_0^2 > 3$, we have the Ree function field $\mathcal{R}$ over $\mathbb{F}_{q^2}$. It is defined by $\mathcal{R} = \mathbb{F}_{q^2}(x, y_1, y_2)$, where

$$y_1^q - y_1 = x^{q_0}(x^q - x)$$
$$y_2^q - y_2 = x^{2q_0}(x^q - x).$$

It has genus $\frac{3}{2}q_0(q-1)(q+q_0+1)$ and its automorphism group is isomorphic to the Ree group $R(q)$. The Ree function field is maximal over $\mathbb{F}_{q^6}$.

There is also a class field theoretic description of these three maximal function fields, due to Lauter [53]. Let p be a prime and q be a prime power. Let $F = \mathbb{F}_q(x)$ and P_∞ be the place at infinity corresponding to the pole of x. Then we can characterize the three maximal function fields as the ray class fields of conductor kP_∞ in which all rational places of F except P_∞ split completely, where

$$k = \begin{cases} p^{f/2} + 2 & , q = p^f \text{ is a square. (The Hermitian case)} \\ p^{(f-1)/2} + 2 & , q = 2^f \text{ is not a square. (The Suzuki case)} \\ p^{(f-1)/2} + 3 & , q = 3^f \text{ is not a square. (The Ree case)} \end{cases}$$

In 2009, Giuletti and Korchmáros [29] discovered a new maximal function field $\mathcal{C}_3$, now known as the Giuletti-Korchmáros function field, or the GK function field. This function field is interesting because it cannot be obtained by taking subfields of the above examples. (We will talk about subfields of maximal function fields later in this chapter.) It is defined over $\mathbb{F}_{q^6}$ with $q > 2$ (if $q = 2$ the field is a subfield of the Hermitian function field) by $\mathcal{C}_3 = \mathbb{F}_{q^6}(x,y,z)$, with

$$x^q + x = y^{q+1}$$
$$y^{q^2} - y = z^{\frac{q^3+1}{q+1}}.$$

It has genus $\frac{1}{2}(q-1)(q^4+q^3-q^2)$, and its automorphism group is also found in [29].

The GK function field is generalized in [22] to a family of maximal function fields $\mathcal{C}_n$, called the generalized GK function fields, over $\mathbb{F}_{q^{2n}}$ for any odd $n \geq 3$. They are defined by $\mathcal{C}_n = \mathbb{F}_{q^{2n}}(x,y,z)$ with

$$x^q + x = y^{q+1}$$
$$y^{q^2} - y = z^{\frac{q^n+1}{q+1}}.$$

When $n = 3$ we get back the original GK function field. The genus of $\mathcal{C}_n$ is $\frac{1}{2}(q-1)(q^n+q^{n+1}-q^2)$. The automorphism groups of these generalized GK function fields are found in [33] and [34]. It is not known if there exists a class field theoretic characterization of the GK and the generalized GK function fields similar to that of Lauter [53].

3.4 Subfields of maximal function fields

In the previous section we encountered some examples of maximal function fields. We want to construct more maximal function fields from the existing ones. One method to do this is to consider subfields of a maximal function field. We will first show that such subfields are themselves maximal, and give some methods of constructing them systematically.

Theorem 3.9 (Serre)**.** *Let E be a maximal function field over $\mathbb{F}_{q^2}$, and let F be another function field. If F is a subfield of E that contains $\mathbb{F}_{q^2}$, then F is also maximal.*

Proof. By Proposition 2.19, the L-polynomial of F divides the L-polynomial of E. The L-polynomial of E is $(1+qu)^{2g(E)}$ by Proposition 3.7(1), so the L-polynomial of F must have the same form. Thus F is maximal. □

A method to construct subfields from a function field is by taking quotients. We briefly recall the construction here: if K is a function field with automorphism group $\mathrm{Aut}(K)$, then for any subgroup $G \subseteq \mathrm{Aut}(K)$, the quotient field K^G is the fixed field of K by G. As the automorphism groups of the examples in the previous section are known, we can construct many of their subfields using this method. Many quotients of the Hermitian function fields are found in [13, 12, 26], and we will give some details in the next section. For quotients of other maximal function fields, see [8, 18, 30]. The family of maximal function fields $\mathcal{X}_n = \mathbb{F}_{q^{2n}}(y,z)$ with $n \geq 3$ odd and

$$y^{q^2} - y = z^{\frac{q^n+1}{q+1}} \tag{3.3}$$

is a subfield of the generalized GK function field, but it was proved to be maximal in [1] prior to the construction of the GK function field and its generalization.

Chapter 4

The subcover problem

In this chapter we will talk about the "subcover problem" of the Hermitian function field. In particular, we will show that the generalized GK function field is not a Galois subfield (meaning that the corresponding extension is Galois) of the Hermitian function field. Further directions are also discussed.

4.1 The subcover problem

In the previous chapter, we saw that subfields of maximal function fields are maximal. As the Hermitian function field $\mathcal{H}$ has the largest possible genus for a maximal function field, subfields of $\mathcal{H}$ provide many examples of maximal function fields. In fact, most of the examples we know are subfields of $\mathcal{H}$. In some sense, these examples are already predicted. We are thus interested in finding "new" examples of maximal function fields in the sense that they cannot be obtained as subfields of $\mathcal{H}$. This raises the issue of checking whether a given maximal function field is a subfield of the Hermitian function field.

The subcover problem. Let $\mathcal{H}/\mathbb{F}_{q^2}$ be the Hermitian function field. Given a maximal function field $\mathcal{X}/\mathbb{F}_{q^2}$, determine if $\mathcal{X}$ is a subfield of $\mathcal{H}$.

This problem is in general hard since we know very little about non-Galois subfields. Thus we will also consider the easier problem of determining if $\mathcal{X}$ is a *Galois* subfield of $\mathcal{H}$.

So far, the only example of a maximal function field we know that is not a subfield of the Hermitian function field $\mathcal{H}$ is the GK function field $\mathcal{C}_3$ [29]. There are a few more examples of maximal function fields that are not Galois subfields of $\mathcal{H}$ (but we do not know if they are subfields of $\mathcal{H}$). The first such example is given by Garcia and Stichtenoth [24] where the field $\mathcal{Y} = \mathbb{F}_{3^6}(y, z)$ with $y^9 - y = z^7$. The field $\mathcal{Y}$ is a special case of the function field $\mathcal{X}_n = \mathbb{F}_{q^{2n}}(y, z)$ with

$$y^{q^2} - y = z^{\frac{q^n+1}{q+1}} \tag{4.1}$$

over $\mathbb{F}_{q^{2n}}$, for $q \geq 2$ and odd $n \geq 3$. We have $g(\mathcal{X}_n) = \frac{1}{2}(q-1)(q^n-q)$. For $n = 3$, $\mathcal{X}_n$ is a subfield of $\mathcal{H}$ when

$q = 2$ (see [1]), and the result of Garcia and Stichtenoth corresponds to the case $q = 3$. An unpublished work of Rains and Zieve shows that the Ree function field for $q = 3$ is another example of a maximal function field not being a Galois subfield of $\mathcal{H}$. In this chapter, we show that the generalized GK function fields and some special examples of the $\mathcal{X}_3$ are also not Galois subfields of $\mathcal{H}$.

Theorem 4.1. *The generalized GK function field $\mathcal{C}_n$, defined by (3.3) over $\mathbb{F}_{q^{2n}}$, is not a Galois subfield of the Hermitian function field $\mathcal{H}_n$ over $\mathbb{F}_{q^{2n}}$ for any $q \geq 3$ and odd $n \geq 3$. For $q = 2$ and odd $n \geq 5$, if $\mathcal{C}_n$ is a Galois subfield of $\mathcal{H}_n$, then the extension $\mathcal{H}_n/\mathcal{C}_n$ is unramified and has degree $d = (2^n + 1)/3$.*

Theorem 4.2. *If $q = p$ is a prime, the maximal function field $\mathcal{X}_3$ defined over $\mathbb{F}_{q^6}$ by the equation*

$$x^{q^2} - x = y^{\frac{q^3+1}{q+1}}$$

is not a Galois subcover of the Hermitian function field over the same finite field.

We remark that we do not know if these function fields are (non-Galois) subfield of the Hermitian function field.

4.2 The degree of a subfield of the Hermitian function field

Suppose we are given two (not necessarily maximal) function fields E and F. If F is a subfield of E, we can consider the degree of extension $d = [E : F]$. Our first job in this section is to obtain some bounds on d. First, the Hurwitz genus formula (Theorem 2.12) gives an upper bound for d.

$$d \leq \frac{g(E) - 1}{g(F) - 1}.$$

The equality holds if and only if the different $\mathrm{Diff}(E/F)$ is zero, in other words if the extension E/F is unramified. On the other hand, by considering the splitting of rational places, we have a lower bound for d.

$$d \geq \frac{N(E)}{N(F)}.$$

The equality holds if and only if every rational place in E/F split completely. Combining the two bounds, we have

$$\frac{N(E)}{N(F)} \leq d \leq \frac{g(E) - 1}{g(F) - 1}. \tag{4.2}$$

Example 4.3. As an example, we show that the GK function field $\mathcal{C}_3$ is not a subfield of the Hermitian

function field $\mathcal{H}_3$ (both over q^6) for $q > 2$. We have

$$g(\mathcal{H}_3) = q^3(q^3-1)/2,$$
$$g(\mathcal{C}_3) = \frac{1}{2}(q-1)(q^4+q^3-q^2).$$

As both function fields are maximal, we have

$$N(\mathcal{H}_3) = q^6 + 1 + 2q^3 g(\mathcal{H}_3) = q^9 + 1,$$
$$N(\mathcal{C}_3) = q^8 - q^6 + q^5 + 1.$$

The bounds (4.2) say

$$\frac{q^9+1}{q^8-q^6+q^5+1} \leq d \leq \frac{q^3-2}{q^2-2}.$$

Since d is an integer, this is impossible for $q > 2$. Therefore, the GK function field is not a subfield of the Hermitian function field. When $q = 2$, the above inequalities give $d = 3$. In this case, the GK function field is actually a subfield of the Hermitian function field: use the description of $\mathcal{H}_3 = \mathbb{F}_{q^6}(u, v)$ with $u^{q^3+1} + v^{q^3+1} + 1 = 0$, and combine the two defining equations of $\mathcal{C}_3$ to give

$$z^{q^3+1} = x^{q^3} + x - (x^q + x)^{q^2-q+1}. \tag{4.3}$$

The field $K = \mathbb{F}_{q^6}(x, z)$ with x, z satisfying (4.3) is the same as $\mathcal{C}_3$. Now take any primitive cube root of unity ω and set

$$X = \omega + \frac{u^3}{u^3+v^3}, \qquad Z = \frac{uv}{u^3+v^3}.$$

These are degree 3 functions as predicted by (4.2). One easily checks that X, Z satisfy (4.3) for $q = 2$ and hence $\mathcal{C}_3$ is a subfield of $\mathcal{H}_3$ when $q = 2$.

In view of proving Theorem 4.1, now we specialize (4.2) to the case when $E = \mathcal{H}_n$ is the Hermitian function field over $\mathbb{F}_{q^{2n}}$ and F is a maximal function field of genus g. So,

$$g(\mathcal{H}_n) = \frac{1}{2}q^n(q^n-1), \qquad N(\mathcal{H}_n) = q^{3n}+1,$$
$$g(F) = g, \qquad N(F) = q^{2n} + 1 + 2gq^n = (q^n+1)^2 + (2g-2)q^n.$$

Note that $2g(\mathcal{H}_n) - 2 = (q^n - 2)(q^n + 1)$. For $(A-1)(q^n+1) \leq 2g-2 < A(q^n+1)$, the bounds (4.2) yield

$$\frac{q^n}{A+1} \leq d \leq \frac{q^n - 2}{A-1}.$$

The lower bound holds with equality for a subfield $\mathcal{Y}_n \subseteq \mathcal{H}_n$ of degree d with

$$2g(\mathcal{Y}_n) - 2 = (q^n/d - 1)(q^n + 1) - (q^n/d + 1) \tag{4.4}$$

for $d|q^n$. Such a subfield exists for every divisor d of q^n ([26, Section 3]). For other cases we will use the following refinement of the lower bound.

Lemma 4.4. *Let F be a maximal function field of genus g, and let $2g-2 = A(q^n+1) - B$ for integers A and B with $1 \leq B \leq q^n + 1$. For $k(A+1) < B$, and for $B \neq A+2$,*

$$\frac{q^n + k}{A+1} \leq d.$$

In particular, $d(A+1) \geq q^n + 1$ for $B > A+2$.

Proof. For the relevant case $B = k(A+1)+1$, the inequality $N(\mathcal{H}_n)(A+1) > N(F)(q^n - 1 + k)$ reduces to $(kq^n - 1)(k-2) + A + A(k-1)^2 q^n > 0$, which holds for $k \geq 2$ and for $k = 0$. For $k = 1$, we need to verify only the case $B = A+3$. For $B = A+3$, the inequality $N(\mathcal{H}_n)(A+1) > N(F)(q^n)$ reduces to $q^{2n} - q^n + A + 1 > 0$. □

By Hurwitz genus formula, if $R = \mathrm{Diff}(\mathcal{H}_n/F)$, we have

$$2g(\mathcal{H}_n) - 2 = d(2g-2) + \deg R.$$

Let k be the largest integer with $k(A+1) < B$. For the degree of the ramification divisor R we write

$$\deg R = (2g(\mathcal{H}_n) - 2) - d(2g-2) = R_0(q^n+1) + R_1, \tag{4.5}$$

where $R_0 = (q^n - 2 - dA + k)$ and $R_1 = dB - k(q^n+1)$.

If the extension $\mathcal{H}_n/F$ is Galois, one can write $\deg R$ in a different way using Theorem 2.13. Information about the $i(\sigma)$ appearing in that theorem can be obtained by analyzing the Artin representation of $G = \mathrm{Aut}(\mathcal{H}_n) = PGU(3, q^n)$. In many cases, we can improve the lower bound in Lemma 4.4 further.

4.3 Artin representation

Before we define the Artin representation, we recall very briefly some basics of representation theory of finite groups. For more details, see [73]. Let G be a finite group. A *class function* on G is a map $f : G \to \mathbb{C}$ such that $f(s) = f(tst^{-1})$ for all $t, s \in G$. Let V be a complex, finite dimensional vector space, and let $GL(V)$ be the automorphism group of V (so that $GL(V) \cong GL_n(\mathbb{C})$, where n is the dimension of V). A *representation* of G in V is a homomorphism $\rho : G \to GL(V)$. Two representations ρ, ρ' in V are *isomorphic* if there is an automorphism τ of V such that $\tau \circ \rho(s) = \rho'(s) \circ \tau$ for all $s \in G$.

If $s \in G$, then $\rho(s)$ is a linear map from V to itself, and we can speak of its trace. The *character* of the representation ρ is a class function defined by

$$\chi_\rho(s) = \mathrm{Tr}(\rho(s)).$$

The character is important since it determines ρ up to isomorphism. The *degree* (or the *dimension*) of ρ is $\chi_\rho(1)$, which is the dimension of V.

The trivial character $\chi(s) = 1$ for all $s \in G$ corresponds to the trivial representation, which we denote by 1_G. It has degree 1. Let $V = \mathbb{C}G$ be the complex group algebra of G, which is a complex vector space of dimension $|G|$ with a basis $(e_s)_{s \in G}$ indexed by the group elements. For $t \in G$, let $\rho_s : V \to V$ be the linear map sending e_s to e_{ts}. This defines a representation called the *regular representation*, with character denoted by r_G. We have $r_G(1) = |G|$ and $r_G(s) = 0$ for all $s \neq 1$ in G. The trivial representation is a subrepresentation of the regular representation. The quotient is called the *augmented representation*, with its character denoted by u_G. We have $r_G = 1_G + u_G$.

A character is *irreducible* if the corresponding representation is irreducible, i.e. it cannot be written as direct sums of proper subrepresentations. If f_1, f_2 are two class functions on G, define the inner product

$$(f, g) = \frac{1}{|G|} \sum_{s \in G} f(s)\overline{g(s)}.$$

It can be shown that the irreducible characters form an orthonormal basis for the space of class functions.

If H is a subgroup of G, and ρ is a representation of H, the induced representation of ρ of G, denoted by ρ^*, is defined by

$$\rho^*(s) = \sum_{t \in G/H} \rho(tst^{-1})$$

for all $s \in G$, with the convention that $\rho(tst^{-1}) = 0$ if $tst^{-1} \notin H$.

We are now ready to define the Artin representation. First let L/K be a finite Galois extension of local

complete fields with Galois group G. Let f be the degree of the residue field extension. Let π be a local uniformizer in L and $\sigma \in G$, set

$$i_G(\sigma) = v_L(\sigma\pi - \pi).$$

Consider the function a_G defined by

$$a_G(\sigma) = -f \cdot i_G(\sigma) \quad \text{if } \sigma \neq 1,$$
$$a_G(1) = f \sum_{\sigma \neq 1} i_G(\sigma).$$

Thus $(a_G, 1_G) = 0$ and $a_G(\sigma) \leq 0$ for all $\sigma \neq 1$. It can be shown (highly nontrivial though) that the function a_G is the character of a representation of G. This representation is called the *Artin representation* in the local case, and a_G is called the *Artin character*.

In the global case, assume that L/K is Galois with separable residue field extensions. Fix a place P in K and let $\mathfrak{P}$ be one of its extensions in L. Let $L_{\mathfrak{P}}/K_P$ be the corresponding local extension, and denote by $\hat{L}_{\mathfrak{P}}, \hat{K}_P$ the completion of $L_{\mathfrak{P}}, K_P$ respectively. The extension $\hat{L}_{\mathfrak{P}}/\hat{K}_P$ is Galois with group $D_{\mathfrak{P}}$, the decomposition group of $\mathfrak{P}|P$. In this extension we can talk about the Artin representation $a_{\mathfrak{P}}$ as in the local case, and the Artin representation of L/K at P is the sum

$$a_P = \sum_{\mathfrak{P}|P} a_{\mathfrak{P}}$$

It can be shown that a_P is the induced representation $(a_{\mathfrak{P}})^*$ for any $\mathfrak{P}$ above P, and does not depend on the choice of $\mathfrak{P}$ above P. Finally, the Artin representation of L/K is the direct sum of the Artin representations at various P.

$$a_{L/K} = \sum_{P \in \mathbb{P}_K} a_P.$$

The relation between the Artin representation and the $i(\sigma)$ defined in (2.5) is clear by their definitions. We have $a_{L/K}(\sigma) = -i(\sigma)$ for any $\sigma \neq 1$ in G. In the case of subfields of the Hermitian function field $\mathcal{H}_n$ over $\mathbb{F}_{q^{2n}}$ and $G = \mathrm{Aut}(\mathcal{H}_n) = \mathrm{PGU}(3, q^n)$, the Artin representation is the unique nontrivial irreducible representation of minimal degree $2g(\mathcal{H}_n) = q^n(q^n - 1)$ (see [50, Lemma 4.1]). Theoretically, we can obtain some information of the $i(\sigma)$ by representation theory, but we will go the opposite way and obtain some information of the Artin character using some projective geometry of $\mathcal{H}_n$.

4.4 Artin character of the Hermitian function field

In this section, we investigate the values of $i(\sigma)$ defined by (2.5) for $\sigma \in PGU(3, q^n)$. The group $PGU(3, q^n)$ has order $q^{3n}(q^{3n}+1)(q^{2n}-1)$, and the action of $PGU(3, q^n)$ on the Hermitian function field $\mathcal{H}_n$ is well-known [79]. An element in $PGU(3, q^n)$ either fixes no places on $\mathcal{H}_n$, or it fixes a place of degree one, or fixes a place of degree three. If σ fixes no places on $\mathcal{H}_n$, then $i(\sigma) = 0$. If it fixes a place of degree three, then it fixes only that place. Since any such σ has order dividing $q^{2n} - q^n + 1$, which is relatively prime to q, the ramification is tame. Hence $i(\sigma) = 3$. The case when σ fixes a place of degree one has several subcases. Since $PGU(3, q^n)$ acts transitively on the degree one places on $\mathcal{H}_n$ (see for example [45]), and $i(\sigma)$ is unchanged under conjugation by Proposition 2.14(1), we may assume that the degree one place fixed is the place at infinity P_∞, the place corresponding to the pole of x when $\mathcal{H}_n$ is defined by the equation

$$y^{q^n} + y = x^{q^n+1}. \tag{4.6}$$

Let H be the subgroup of $PGU(3, q^n)$ fixing P_∞. One can show that H is of order $q^{3n}(q^{2n}-1)$, and any $\sigma \in H$ is of the form

$$\sigma(x) = a^{q^n+1}x + ab^{q^n}y + c, \qquad \sigma(y) = ay + b, \tag{4.7}$$

with $a \in \mathbb{F}_{q^{2n}} \backslash \{0\}$, $b \in \mathbb{F}_{q^{2n}}$, $c^{q^n} + c = b^{q^n+1}$. Following the notations in [26], we denote by $\sigma = [a, b, c]$ the automorphism $\sigma \in H$ given by (4.7). There are 2 cases.

Lemma 4.5. *Let P_∞ be the pole of x when $\mathcal{H}_n$ is defined by (4.6), and let H be the subgroup of $PGU(3, q^n)$ fixing P_∞. Let $\sigma = [a, b, c] \in H$ with $\sigma \neq 1$. For $a \neq 1$, we have (here $p = char(\mathcal{H}_n)$)*

$$i(\sigma) = \begin{cases} 1 & , \text{ if } p \text{ divides } \mathrm{ord}(\sigma), \\ q^n + 1 & , \text{ if } \mathrm{ord}(\sigma) \text{ divides } q^n + 1, \\ 2 & , \text{ otherwise.} \end{cases}$$

For $a = 1$, we have

$$i(\sigma) = \begin{cases} 2 & , \text{ if } a = 1, b \neq 0, \\ q^n + 2 & , \text{ if } a = 1, b = 0, c \neq 0. \end{cases}$$

Proof. (Case $a \neq 1$) The Sylow p-subgroup of H is the set consisting of $[a, b, c]$ with $a = 1$. Therefore, if $\sigma = [a, b, c]$ with $a \neq 1$, then σ is not in the higher ramification group of P_∞, so it will not fix P_∞ to a high

order. Since all other places are at most tamely ramified, we have

$$i_P(\sigma) = v_P(\sigma(t) - t) = \begin{cases} 0 & , \sigma(P) \neq P, \\ 1 & , \sigma(P) = P. \end{cases}$$

Therefore, in this case we have

$$i(\sigma) = \#\{P \in \mathcal{H}_n | \deg(P) = 1 \text{ and } \sigma(P) = P\}.$$

If $\mathrm{ord}(\sigma)$ is a multiple of p, then σ does not fix any degree one places other than P_∞ since those places are tame. Thus $i(\sigma) = 1$. Suppose now $\mathrm{ord}(\sigma)$ divides $q^n + 1$, then one can show that $\sigma = [a, b, c]$ is conjugate in H to $\sigma^* = [a, 0, 0]$ (see [26, Lemma 4.1]). By (4.7), σ^* satisfies $\sigma^*(x) = x$ and $\sigma^*(y) = ay$. It is then easy to see that apart from P_∞, σ^* fixes exactly the q^n places above $(y = 0)$. Hence, $i(\sigma^*) = q^n + 1$ as σ^* also fixes P_∞. Since $i(\sigma)$ is preserved under conjugation, we have $i(\sigma) = i(\sigma^*) = q^n + 1$. Finally, if the order of σ does not divide $q^n + 1$, then again $\sigma = [a, b, c]$ is conjugate in H to $\sigma^* = [a, 0, 0]$. This time we have $\sigma^*(x) = a^{q^n+1}x$ and $\sigma^*(y) = ay$. So apart from P_∞, σ^* fixes exactly the place at the origin $(x = 0, y = 0)$. Thus $i(\sigma) = i(\sigma^*) = 2$.

(Case $a = 1$) If $\sigma = [a, b, c]$ with $a = 1$, then σ is in the higher ramification group of P_∞, and this is the unique place fixed by σ. In this case, we compute $i(\sigma)$ directly from the definition. First, $i(\sigma) = i_{P_\infty}(\sigma) = v_{P_\infty}(\sigma(t) - t)$, where t is a local uniformizer at P_∞. We choose $t = y/x$ to be the local uniformizer. Then

$$\begin{aligned} i(\sigma) &= v_{P_\infty}\left(\frac{y+b}{x + b^{q^n}y + c} - \frac{y}{x}\right) \\ &= v_{P_\infty}((y+b)x - y(x + b^{q^n}y + c)) - v_{P_\infty}(x) - v_{P_\infty}(x + b^{q^n}y + c) \\ &= v_{P_\infty}(-b^{q^n}y^2 + bx - cy) + 2(q^n + 1) \\ &= \begin{cases} 2 & , \text{ if } b \neq 0, \\ q^n + 2 & , \text{ if } b = 0, c \neq 0. \end{cases} \end{aligned}$$

□

The $i(\sigma)$ for various kinds of elements are shown in Figure 4.1. Each number in a box corresponds to a subgroup of that order, and each number on an edge is the $i(\sigma)$ for elements that lie in the upper group but not the lower one.

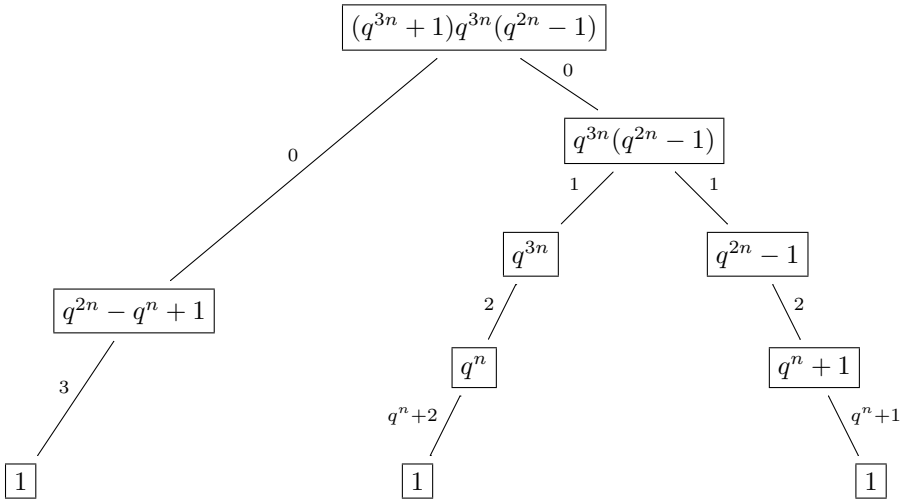


Figure 4.1: $i(\sigma)$ among various elements in $PGU(3, q^n)$

The following proposition follows immediately from the above lemma. The significance of the proposition is that either $i(\sigma)$ is very small, or it is very large, and nothing in the middle can happen.

Proposition 4.6. *If $\sigma \in PGU(3, q^n)$, then $i(\sigma) = 0, 1, 2, 3, q^n + 1$ or $q^n + 2$.*

Now we have the contribution of each element in $PGU(3, q^n)$ to the ramification divisor. By contrasting the formula of $\deg R$ in Theorem 2.13 and (4.5), we can improve the lower bound in Lemma 4.4 further in the Galois case. This will be done in the next section.

4.5 Improved lower bound in the Galois case

In Theorem 2.13, we write the degree of the ramification divisor R as the sum of $i(\sigma)$ for the $d-1$ nontrivial σ in the Galois group G, and in Proposition 4.6 we found the possible values for each $i(\sigma)$. In particular, the nontrivial elements divide into two groups according to $i(\sigma) = 0, 1, 2, 3$ or $i(\sigma) = q^n + 1, q^n + 2$. Write $d = 1 + u + v$ with

$$u = \#\{\sigma \neq 1 : i(\sigma) = 0, 1, 2, 3\} \quad \text{and} \quad v = \#\{\sigma \neq 1 : i(\sigma) = q^n + 1, q^n + 2\}.$$

Then

$$v(q^n + 1) \leq \deg R \leq v(q^n + 1) + 3u + v. \tag{4.8}$$

For a subfield F of the Hermitian function field $\mathcal{H}_n$, not necessarily Galois, let $2g(F) - 2 = A(q^n + 1) - B$, with $1 \leq B \leq q^n + 1$, and let k be the largest integer with $k(A + 1) < B$. As in (4.5), let

$$\deg R = (2g(\mathcal{H}_n) - 2) - d(2g(F) - 2) = R_0(q^n + 1) + R_1, \tag{4.9}$$

where $R_0 = (q^n - 2 - dA + k)$ and $R_1 = dB - k(q^n + 1)$. Clearly,

$$k(R_0 - d) + (R_1 - d) \geq k(k - 3). \tag{4.10}$$

We will now prove a new lower bound for d.

Proposition 4.7. *Let F be a maximal function field with $2g(F) - 2 = A(q^n + 1) - B$, for integers A and B with $1 \leq B \leq q^n + 1$. For $B > A + 2$ and for $k(A + 1) < B$, if $\mathcal{H}_n/F$ is a Galois extension of degree d, then $dB \geq (k + 1)(q^n + 1)$.*

Proof. Assume to the contrary that $dB < (k + 1)(q^n + 1)$. Since $B \geq 2k + 1$, $3d < 2(q^n + 1)$, and thus $3u + v < 2(q^n + 1)$. With Lemma 4.4, $dB > dk(A + 1) \geq k(q^n + 1)$. Together with the assumption,

$$k(q^n + 1) < dB < (k + 1)(q^n + 1).$$

For $\deg R = R_0(q^n + 1) + R_1$ in (4.9), it follows that R_0 corresponds to the quotient and R_1 to the remainder after divisor by $q^n + 1$. Now we compare with (4.8). Using $R_0 \leq v + 1$ and $R_1 \leq 3u + v$,

$$k(R_0 - d) + (R_1 - d) \leq k(-u) + 2u - 1,$$

which, for $k \geq 3$, contradicts (4.10). It remains to prove the case $(k = 2)$ and the case $(k = 1, B > A + 2)$. Observe that for $(k = 1, B > A + 2)$, (4.10) can be replaced with

$$(R_0 - d) + (R_1 - d) \geq d - 2. \tag{4.11}$$

If $3u + v < q^n + 1$ then $R_0 = v$ and $R_1 \leq 3u + v$. For $(k = 2)$, $2R_0 + R_1 \leq 3u + 3v = 3d - 3$ contradicts (4.10). For $(k = 1, B > A + 2)$, $R_0 + R_1 \leq 3u + 2v = 2d + u - 2$ contradicts (4.11). If $3u + v \geq q^n + 1$ then $R_0 \leq v + 1$ and $R_1 \leq 3u + v - 1$. For $(k = 2)$, $2R_0 + R_1 \leq 3u + 3v + 1 = 3d - 2$. In combination with (4.10) equality holds and $R_0 = v + 1$ and $R_1 = 3u + v - 1$. The latter implies $3u + v = q^n + 1$, and $R_0 = v + 1$ would then imply $R_1 = 0$, a contradiction. For $(k = 1, B > A + 2)$, $R_0 + R_1 \leq 3u + 2v = 2d + u - 2$ contradicts

(4.11). □

4.6 Proof of Theorem 4.1 and 4.2

We will apply Proposition 4.7 to the generalized GK function field $\mathcal{C}_n$ and the function field $\mathcal{X}_n$ defined by (3.3), that are both maximal over $\mathbb{F}_{q^{2n}}$. For their genera we have

$$\begin{aligned} 2g(\mathcal{H}_n) - 2 &= (q^n - 2)(q^n + 1), \\ 2g(\mathcal{C}_n) - 2 &= (q^2 - 1)(q^n + 1) - (q^3 + 1), \qquad (4.12) \\ 2g(\mathcal{X}_n) - 2 &= (q - 1)(q^n + 1) - (q^2 + 1). \qquad (4.13) \end{aligned}$$

We first consider the generalized GK function field $\mathcal{C}_n$. Suppose now that $\mathcal{H}_n/\mathcal{C}_n$ is a Galois extension of degree d. From (4.12), we have $A = q^2 - 1$, $B = q^3 + 1$ and $k = q$. Proposition 4.7 gives the lower bound for d as

$$d \geq \frac{(k+1)(q^n+1)}{B} = \frac{q^n+1}{q^2-q+1}.$$

From (4.2) we have the upper bound, for $n \geq 3$,

$$d \leq \frac{2g(\mathcal{H}_n) - 2}{2g(\mathcal{C}_n) - 2} \leq \frac{q^n - 2}{q^2 - 2}.$$

For $q \geq 3$ and $n \geq 3$ the lower bound exceeds the upper bound and no solutions for d exist. Hence the generalized GK function cannot be a Galois subfield of the Hermitian function field. This is the case $q \geq 3$ for Theorem 4.1.

For $q = 2$, $2g(\mathcal{H}_n) - 2 = (2^n + 1)/3 \cdot (2g(\mathcal{C}_n) - 2)$ and the inequalities admit the unique solution $d = (2^n + 1)/3$. In this case, the ramification divisor is zero. Thus the Galois extension $\mathcal{H}_n/\mathcal{C}_n$, if it exists, has to be unramified. This proves the case $q = 2$ of Theorem 4.1.

Remark 4.8. In the case $q = 2$ (and odd $n \geq 5$) it is easy to write down some possible unramified quotients of $\mathcal{H}_n$ of degree $d = (2^n + 1)/3$ that have the correct genus. However, it is not clear if any one of those possibilities will give a quotient that is isomorphic to the GK function field. Due to the fact that there exists a similar family of quotients having the same genus, same ramification structure below the Hermitian function field, same automorphism group, and the same Weierstrass semigroup on a generic place, but yet are not isomorphic to each other [28], this type of question has to be studied very carefully.

Remark 4.9. In the proof we did not use the fact that we are dealing with the generalized GK function field

$\mathcal{C}_n$. What we use is only the genus of $\mathcal{C}_n$ given by (4.12). Thus we actually proved that there are no function fields with genus $\frac{1}{2}(q-1)(q^{n+1}+q^n-q^2)$ being a Galois subfield of the Hermitian function field $\mathcal{H}_n$ when $q \geq 3$ and odd $n \geq 3$.

We now turn our attention to $\mathcal{X}_n$. Suppose that $\mathcal{H}_n/\mathcal{X}_n$ is a Galois extension of degree d. From (4.13), we have $A = q-1$, $B = q^2+1$ and $k = q$. Proposition 4.7 and (4.2) gives the lower and upper bounds for d as

$$\frac{(q+1)(q^n+1)}{q^2+1} \leq d \leq q^{n-1}+q^{n-2}+\ldots+q^2+q+2. \tag{4.14}$$

Unlike the case for the generalized GK function field, this range is non-empty, and is quite large in general. We will need other methods to completely remove the possibility of these degrees. For an example that this could be done, we consider the function field $\mathcal{X}_3$, for which the range is not too large. Recall its defining equation

$$x^{q^2}-x = y^{\frac{q^3+1}{q+1}}.$$

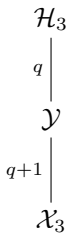
From (4.14), only the three possibilities $d = q^2+q, q^2+q+1$ or q^2+q+2 remain. To analyze the situation further, we may assume $q \geq 4$ since the cases $q = 2, 3$ are known [1, 24].

It is easy to show that q^2+q+2 does not divide the order of $\mathrm{Aut}(\mathcal{H}_3) = (q^9+1)q^9(q^6-1)$ for any q except $q = 2, 3, 10$. Since we are only considering q that are prime powers with $q \geq 4$, we can discard the case $d = q^2+q+2$. For the case $d = q^2+q+1$, $q = p^e$, note that $\mathrm{GCD}(p, q^2+q+1) = \mathrm{GCD}(q^3+1, q^2+q+1) = 1$ for all $q \geq 3$. By the discussion in Section 4.4, any $\sigma \in \mathrm{Aut}(\mathcal{H}_3)$ with $i(\sigma) = q^3+1$ has order dividing q^3+1, and any σ with $i(\sigma) = q^3+2$ has order a power of p. Thus none of the elements σ in the group of order d can have $i(\sigma) = q^3+1$ or q^3+2. This leaves to us $i(\sigma) = 0, 1, 2, 3$. In this case, the ramification divisor R has degree $\deg R = q^4+2q^2+q$. As $3(d-1) < \deg R$, the case $d = q^2+q+1$ is discarded.

The case $d = q^2+q$ is the difficult one. In this case the ramification divisor is $\deg R = 2q^4-q^3+q^2+2q-2$. Suppose $G \subseteq Aut(\mathcal{H}_3) = PGU(3, q^3)$ is a subgroup of order q^2+q. The Sylow p-subgroups in G are all of order q. All Sylow p-subgroups in $PGU(3, q^3)$ are conjugates, and each of them fixes a unique rational place. We may assume that one of the Sylow p-subgroups Q (of order q) of G has P_∞ as its unique fixed place. There are two subcases: either Q is normal (so it is the only Sylow p-subgroup of G), or it is not.

4.6.1 The case when Q is normal

First suppose that Q is normal in G. Let $\mathcal{Y}$ be the fixed field of $\mathcal{H}_3$ by Q. We have the following field extensions over $\mathbb{F}_{q^6}$:



Let P'_∞ be the unique place in $\mathcal{Y}$ below P_∞. In the upper extension, the place P'_∞ is the only ramified place, and is totally ramified. Let P''_∞ be the place in $K(\mathcal{Y})$ below P'_∞, then P''_∞ must be completely ramified in $\mathcal{Y}$ since $\mathcal{Y}$ is Galois over $\mathcal{X}_3$ (we used the fact Q is normal here) and P'_∞ has no conjugates other than itself. Therefore, there is a place P''_∞ in $\mathcal{X}_3$ that is totally ramified in $\mathcal{H}_3$. The following result from [26] is useful.

Lemma 4.10. *Let $q = p^e$ be a prime power, and let $\mathcal{H}$ be the Hermitian function field over $\mathbb{F}_{q^2}$, and let A be the stabilizer of P_∞ in Aut($\mathcal{H}$). Let G be a subgroup of A, and suppose that $\mathcal{H}/\mathcal{X}$ is a Galois extension over $\mathbb{F}_{q^2}$ with Galois group G. Write*

$$|G| = \deg \phi = m \cdot p^u \text{ with } GCD(m, p) = 1.$$

Then the genus of the fixed field $\mathcal{X}$ is given by

$$g(\mathcal{X}) = \frac{q - p^w}{2m \cdot p^u}(q - (d-1) \cdot p^v),$$

where $d = GCD(m, q+1)$ and $v, w \geq 0$ are some integers depend on G such that $v + w = u$.

Proof. This is a combination of Theorem 2.2, Section 3 and Theorem 4.4 of [26]. □

In our case $d = |G| = q(q+1) = (q+1)p^e$ (note that our q here is different from the one in Lemma 4.10, the q there is q^3 in our situation). Suppose $\mathcal{X}$ is a Galois subcover of $\mathcal{H}_3$ of degree d, we have

$$g(\mathcal{X}) = \frac{q^3 - p^w}{2(q+1)}(q^3 - ((q+1) - 1) \cdot p^v) = \frac{p^{3e} - p^w}{2(p^e+1)}(p^{2e} - p^v),$$

where $v + w = e$. The only combination that gives an integer value of $g(\mathcal{X})$ is $v = 0, w = e$. In this case we get $g(\mathcal{X}) = \frac{1}{2}(q-1)(q^3 - q)$, which is exactly the genus of $\mathcal{X}_3$ under investigation. By the theory in Section

4 of [26], we can actually write down the $i(\sigma)$ for all $\sigma \in G$, $\sigma \neq 1$, which turns out to be

$i(\sigma)$	0	1	2	3	q^3+1	q^3+2
$\#\sigma$	0	q^2-q	0	0	q	$q-1$

We can even write down one set of defining equations of $\mathcal{X}$. We use the equation $x^{q^3}+x=y^{q^3+1}$ for $\mathcal{H}_3$. From the discussion of Section 4.4, the subgroup of q elements having $i(\sigma)=q^3+2$ is generated by σ_1 with

$$\sigma_1(x)=x+c, \sigma_1(y)=y,$$

with $c^q+c=0$, and the subgroup of $q+1$ elements with $i(\sigma)=q^3+1$ is generated by σ_2 with

$$\sigma_2(x)=x, \sigma_2(y)=ay,$$

where $a^{q+1}=1$. The fixed field $\mathcal{X}$ can be given by the equation

$$X^{q^2}-X^q+X=Y^{\frac{q^3+1}{q+1}}.$$

The uniqueness of σ_1 and σ_2 (up to conjugation) follows from the theory in [26] and arguments similar to Proposition 4.11 below.

To show that we can dispose of this case, it remains to show that the field $\mathcal{X}$ we obtained above is not isomorphic to $\mathcal{X}_3$. This will be done in the following proposition.

Proposition 4.11. *The function fields $\mathcal{X}$ and $\mathcal{X}_3$, with $\mathcal{X}=\mathbb{F}_{q^6}(X,Y)$ and $\mathcal{X}_3=\mathbb{F}_{q^6}(x,y)$ defined by the equations*

$$\mathcal{X}:\ X^{q^2}-X^q+X=Y^{\frac{q^3+1}{q+1}}$$

and

$$\mathcal{X}_3:\ x^{q^2}-x=y^{\frac{q^3+1}{q+1}},$$

are not isomorphic to each other.

Proof. We will mimic the proof in [24] for the case $q=3$. Let P_∞ and Q_∞ be the places at infinity on $\mathcal{X}$ and $\mathcal{X}_3$ respectively. If we have an isomorphism $\phi:\mathcal{X}\to\mathcal{X}_3$, then we must have $\phi(P_\infty)=Q_\infty$ as these places are the only ones with Weierstrass semigroup $\langle\frac{q^3+1}{q+1},q^2\rangle$ (see Satz 6 in [79]). We have the following

pole-divisors

$$\mathrm{div}_\infty(X) = \frac{q^3+1}{q+1}P_\infty, \qquad \mathrm{div}_\infty(Y) = q^2 P_\infty,$$

and

$$\mathrm{div}_\infty(x) = \frac{q^3+1}{q+1}Q_\infty, \qquad \mathrm{div}_\infty(y) = q^2 Q_\infty.$$

Hence we must have constants a, b, c, d, e with $a, d \neq 0$ such that

$$\phi(x) = aX + b, \qquad \phi(y) = cX + dY + e.$$

Using $x^{q^2} - x - y^{\frac{q^3+1}{q+1}} = 0$ we obtain

$$(aX+b)^{q^2} - (aX+b) - (cX+dY+e)^{\frac{q^3+1}{q+1}} = 0.$$

As ϕ is an isomorphism, the equation above has to be a constant multiple of the equation $X^{q^2} - X^q + X - Y^{\frac{q^3+1}{q+1}} = 0$, which is impossible. □

4.6.2 The case when Q is not normal

Now we turn to the case when Q is not normal. We can only treat the case when $q = p$ is a prime. By Sylow theorem, there are exactly $p+1$ subgroups of G of order p. As there are exactly $p+1$ Sylow p-subgroups, and all of them are conjugate, by Proposition 2.14, all nontrivial elements that are inside some Sylow p-subgroup have the same $i(\sigma)$, which can be $0, 1, 2$ or p^3+2. As two distinct Sylow p-subgroups must intersect trivially, there are a total of $(p-1)(p+1) = p^2 - 1$ such elements. As

$$(p^3+2)(p^2-1) > \deg R = 2q^4 - q^3 + q^2 + 2q - 2,$$

these elements cannot have $i(\sigma) = p^3+2$. On the other hand, there are only $p(p+1) - (p^2-1) - 1 = p$ other nontrivial elements τ in G, which may have $i(\tau) = 0, 1, 2, 3$ or p^3+1. However, as $2(p^2-1)+(p^3+1)p < \deg R$ for all $p \geq 3$, we cannot have $i(\sigma) = 0, 1, 2$ either. Therefore, this case does not occur when $p > 3$ is a prime number. This completes the proof of Theorem 4.2.

Remark 4.12. The case when Q is normal works for all $q \geq 3$. When Q is not normal, one may be able to settle the problem if a classification of groups of order $q(q+1)$ is known.

4.7 Conjectures and further remarks

In this section we give some further remarks on the subcover problem, and indicate some possible further directions.

4.7.1 Some conjectures

We start with conjectures on the subcover problem for the generalized GK function field $\mathcal{C}_n$. In view of the case $n = 3$ and Theorem 4.1, the following conjecture seems reasonable.

Conjecture 4.13. *The generalized GK function field $\mathcal{C}_n$ over $\mathbb{F}_{q^{2n}}$ is not a subfield of the Hermitian function field $\mathcal{H}_n$ over the same field for $q \geq 3$ and odd $n \geq 5$. On the contrary, we conjecture that $\mathcal{C}_n$ is a subfield of $\mathcal{H}_n$ for $q = 2$.*

Similarly, for the maximal function field $\mathcal{X}_n$, one may conjecture the following.

Conjecture 4.14. *The field $\mathcal{X}_n$ over $\mathbb{F}_{q^{2n}}$ is not a (Galois) subfield of $\mathcal{H}_n$ for all $q \geq 3$ and odd $n \geq 5$.*

We recall that for $q = 2$, $\mathcal{X}_n$ is known to be a subfield of the Hermitian function field [1].

We may also consider the subcover problems of whether the Suzuki function field or the Ree function field is a subfield of the Hermitian function field. However, their genus is too small compared to that of the corresponding Hermitian function field, and our method in this chapter only gives very weak bounds on the degrees.

4.7.2 Non-Galois subfields

In this subsection we outline a possible way to attack the general (non-Galois) subcover problem. Let $\mathcal{X}$ be a given maximal function field, and let $\mathcal{H}$ be the Hermitian function field, both over the same finite field $\mathbb{F}_{q^2}$. Suppose $\mathcal{H}/\mathcal{X}$ is a non-Galois extension, and let $\overline{\mathcal{H}}$ be the Galois closure. Since $\overline{\mathcal{H}}$ is a proper extension of $\mathcal{H}$, it has a higher genus than the Hermitian function field, and cannot be maximal. Let $n = [\overline{\mathcal{H}} : \mathcal{H}]$, then the number of rational places in $\overline{\mathcal{H}}$ can be bounded by Oesterlé's bound (see [71, Chap. 7]), which is an optimization of Serre's explicit formulas (Proposition 3.4) when both q and g are fixed.

On the other hand, the lower bound (4.2) of the degree $d = [\mathcal{H} : \mathcal{X}]$ is attained when all the rational places in $\mathcal{X}$ splits completely in $\mathcal{H}$. However, a standard algebraic number theory fact states that any place in $\mathcal{X}$ that splits completely in $\mathcal{H}$ will split completely all the way up to the Galois closure (see for example [59, p. 58]). This will violate Oesterlé's bound. Hence the lower bound (4.2) can certainly be improved even in the non-Galois case. The trivial estimation is that for each place P in $\mathcal{X}$, there are at most $d - 1$ places that lie above it. This is certainly a very poor estimation. Can we do better?

Question 4.15. Suppose E/F is a non-Galois extension of function fields with Galois closure K, such that not all places E/F split completely. Can we obtain a non-trivial upper bound for $N(E)$?

If we have a "good" estimate for the above question, then we are able to improve the lower bound in a significant way in the non-Galois case. This may lead to the solution of the subcover problem for the generalized GK function field.

Chapter 5

Generator rank and relation rank

After the study of maximal curves, we change context and investigate the asymptotic behaviour of function fields when their genera goes to infinity. In this and the next two chapters, we will develop the necessary tools for the study. In this chapter, we will define the generator rank and the relation rank and state the Golod-Shafaverich theorem which relates the two ranks.

We start by defining the generator rank and the relation rank.

Definition 5.1. Let p be a prime, and G be a finitely generated pro-p-group. Define the generator rank by

$$d_p(G) = \dim_{\mathbb{F}_p} H^1(G, \mathbb{Z}/p\mathbb{Z}),$$

and the relation rank by

$$r_p(G) = \dim_{\mathbb{F}_p} H^2(G, \mathbb{Z}/p\mathbb{Z}).$$

For a finitely generated profinite group G, let $G' = [G, G]$ be its commutator subgroup, and G^p be the subgroup generated by elements of the form g^p. The p-generator rank (or simply the p-rank) of G is defined by

$$d_p(G) = d_p(G/\overline{G^p G'}),$$

where $\overline{G^p G'}$ is the topological closure of $G^p G'$.

For a finitely generated pro-p-group G, the generator rank and the relation rank has the following group theoretical meaning. We remark that these properties do not hold for a finitely generated profinite group.

Proposition 5.2. *Let G be a finitely generated pro-p-group.*

- *The generator rank $d_p(G)$ is the number of any minimal set of generators of G.*
- *Let $d = d_p(G)$. Suppose we have the short exact sequence*

$$1 \to R \to F \to G \to 1,$$

where F is the free pro-p-group on d generators, then $r_p(G) = d_p(R)$. In other words, $r_p(G)$ is the minimal number of relators of G.

Proof. See [68, Chap. 7]. □

We will need the following lemma to estimate the difference between the relation rank and the generator rank of G.

Lemma 5.3. *Let G be a pro-p-group. If there is a short exact sequence*

$$1 \to H \to G \to \mathbb{Z}/p^n\mathbb{Z} \to 1$$

for some positive integer n, then we have

$$r_p(G) - d_p(G) \leq r_p(H).$$

Proof. See [47]. □

As a corollary, for a p-extension L/K of function fields, and a place $\mathfrak{P}$ in L, denote the inertia group and decomposition group at $\mathfrak{P}$ by $I_{\mathfrak{P}}(L/K)$ and $D_{\mathfrak{P}}(L/K)$ respectively. Then we have the following corollary.

Corollary 5.4.

$$r_p(D_{\mathfrak{P}}(L/K)) - d_p(D_{\mathfrak{P}}(L/K)) \leq r_p(I_{\mathfrak{P}}(L/K)).$$

For an elementary abelian p-group $G = (\mathbb{Z}/p\mathbb{Z})^d$, the generator rank is d, and the relation rank is given by the following lemma.

Lemma 5.5. *Let $G = (\mathbb{Z}/p\mathbb{Z})^d$, then $r_p(G) = \frac{d(d+1)}{2}$.*

Proof. See [47]. □

We end this chapter by stating the Golod-Shafarevich theorem that relates the generator rank and relation rank of a finite group G. The theorem was first proved by Golod and Shafarevich [31] and then improved by Gaschütz and Vinberg (see [27]). The following theorem is the version of Gaschütz-Vinberg.

Theorem 5.6 (Golod-Shafarevich)**.** *Let p be a prime. For every finite nontrivial p-group G, we have*

$$r_p(G) > \frac{d_p(G)^2}{4}.$$

Remark 5.7. Golod-Shafarevich theorem is not true for an infinite pro-p-group G. We will utilize this fact later to check if a certain Galois group is infinite.

Chapter 6

Class field theory of function fields

We collect some facts in class field theory of function fields in this chapter. The main references are [59, 66, 69].

6.1 Ramification groups, conductors and ray class fields

Let K be a complete valued field with respect to a normalized valuation v_K. Let L/K be a finite Galois extension with group G, and v_L be the normalized valuation of L. Let $\mathcal{O}_K$ and $\mathcal{O}_L$ be the corresponding valuation rings of K and L. For each integer $i \geq -1$, the *i-th ramification group* $G_i(L/K)$ is defined as

$$G_i(L/K) = \{\sigma \in G : v_L(\sigma a - a) \geq i + 1 \ \forall a \in \mathcal{O}_L\}.$$

Note that $G_{-1}(L/K) = G$ and G_0 is the inertia group of L/K. In the global case, let L/K be a Galois extension of global fields with Galois group G. For every extension of places $\mathfrak{P}|\mathfrak{p}$ of L/K, we have the local field extension $L_{\mathfrak{P}}/K_{\mathfrak{p}}$. We define the i-th ramification group $G_{i,\mathfrak{P}}$ of L/K at $\mathfrak{P}$ by

$$G_{i,\mathfrak{P}} = G_i(L_{\mathfrak{P}}/K_{\mathfrak{p}}).$$

The ramification groups of index -1, 0 are the decomposition group and the inertia group at $\mathfrak{P}$, respectively. The groups G_i induce a filtration of the decomposition group D of $\mathfrak{P}$. We have the following lemma for the successive quotient of this filtration.

Lemma 6.1. *Let L/K be Galois with group G, $\mathfrak{P}$ be a place of L, and let $l_{\mathfrak{P}}/k_{\mathfrak{p}}$ the residue field extension at $\mathfrak{P}$. Let π be a uniformizer at $\mathfrak{P}$, the maps*

$$\begin{aligned} G_0/G_1 \to l_{\mathfrak{P}}^*, \qquad & \sigma \mapsto \frac{\sigma\pi}{\pi} \mod \mathfrak{P}, \\ G_i/G_{i+1} \to l_{\mathfrak{P}}, \qquad & \sigma \mapsto \frac{\sigma\pi - \pi}{\pi^{i+1}} \mod \mathfrak{P}, i \geq 1, \end{aligned}$$

are injective.

Proof. See [59, p. 177]. □

In particular, G_1 is the unique Sylow p-subgroup of G_0.

For a real number $u \geq -1$, we adopt the convention $G_{u,\mathfrak{P}} = G_{[u]+1,\mathfrak{P}}$. Let g_i be the order of $G_{i,\mathfrak{P}}$. We define a function $\phi = \phi_{L/K,\mathfrak{p}} : [-1,\infty) \to [-1,\infty)$ by

$$\phi(u) = \begin{cases} u & , -1 \leq u \leq 0, \\ \frac{1}{g_0}(g_1 + g_2 + \cdots + g_{[u]} + (u - [u])g_{[u]+1} & , u > 0. \end{cases} \tag{6.1}$$

Note that this definition does not depend on the particular $\mathfrak{P}$ above $\mathfrak{p}$. The function ϕ is continuous, piecewise linear, strictly increasing and concave on $[-1,\infty)$. Therefore it has an inverse ψ, which is continuous, piecewise linear, strictly increasing and convex on $[1,\infty)$.

Lemma 6.2. *We have $\psi(u) \geq u$, and if u is an integer, $\psi(u)$ is an integer.*

Proof. The first part is equivalent to that $\phi(u) \leq u$, which is clear. The second part is [66, Lemma 2.3.2]. □

For all real numbers $v \geq -1$, we define the *upper numbering* of the ramification groups by

$$G^v_{\mathfrak{P}} = G_{\psi_{L/K,\mathfrak{p}}(v)}.$$

Equivalently, $G^{\phi(u)} = G_u$.

The lower ramification numbers behave well under subgroups of the Galois group, and the upper ramification numbers behave well under quotients.

Lemma 6.3. *Let $L/K'/K$ be field extensions, and $\mathfrak{P}|\mathfrak{p}'|\mathfrak{p}$ be the corresponding extensions of a place $\mathfrak{p}$ in K. For all $u, v \geq -1$, we have*

$$G_{u,\mathfrak{P}}(L/K') = G_{u,\mathfrak{P}}(L/K) \cap \mathrm{Gal}(L/K').$$

If L'/K is a Galois subextension of L/K, $\mathfrak{P}|\mathfrak{P}'|\mathfrak{p}$ be the corresponding extensions of $\mathfrak{p}$, and if L/K has separable residue extensions, then

$$G^v_{\mathfrak{P}}(L/K)\,\mathrm{Gal}(L/L')/\,\mathrm{Gal}(L/L') = G^v_{\mathfrak{P}'}(L'/K).$$

Proof. See [59, §II.10]. □

An integer u is called a *lower ramification jump* at $\mathfrak{P}$ if $G_{u,\mathfrak{P}} \neq G_{u+1,\mathfrak{P}}$. The corresponding value $\phi(u)$ in the upper numbering is called an *upper ramification jump* at $\mathfrak{P}$. If the extension is abelian, we have the following.

Theorem 6.4 (Hasse-Arf)**.** *If L/K is abelian, then all the upper ramification jumps are integers.*

Proof. See [74, p.76]. □

From now on, we assume that L/K is a finite abelian extension. The *ramification depth* of a Galois extension L/K at $\mathfrak{p}$ is the least integer $c_{\mathfrak{p}}$ such that $G_{\mathfrak{P}}^{c_{\mathfrak{p}}} = 1$ for all places $\mathfrak{P}$ lying above $\mathfrak{p}$. Thus $\mathfrak{p}$ is unramified in L if $c_{\mathfrak{p}} = 0$, tamely ramified if $c_{\mathfrak{p}} = 1$, and wildly ramified if $c_{\mathfrak{p}} \geq 2$. The *conductor* of the extension L/K is the divisor

$$\mathrm{cond}(L/K) = \sum_{\mathfrak{p} \in \mathbb{P}_K} c_{\mathfrak{p}} \mathfrak{p}.$$

It is clear that the support of $\mathrm{cond}(L/K)$ is precisely the set of all places in K that ramify in L.

We can reverse the above process. Choose a divisor $D = \sum_{\mathfrak{p}} a_{\mathfrak{p}} \mathfrak{p}$ and a non-empty finite set T of places disjoint from the support of D. Define the *T-ray class field* K_T^D of K with ray modulus (or simply modulus) D to be the maximal abelian extension of K that has conductor D and such that all places in T split. The existence of ray class field is guaranteed by class field theory (See [66, Chap. 2]). It can be shown that K_T^D is a finite geometric extension of K with conductor D, and all places in T splits. The Galois group of the extension K_T^D/K is the T-ray class group $Cl_T^D(K)$ of modulus D. It is clear that if D_1, D_2 are two effective divisors whose supports are disjoint from T, then $K_T^{D_1} \subseteq K_T^{D_2}$ if and only if $D_1 \leq D_2$.

Remark 6.5. We require that T is non-empty in order to ensure that the ray class field has the same constant field as K. (We remind the reader that all of our constant fields are finite. The previous statement is in general not true for function fields over other fields.) Let k be the constant field of K and $\bar{k}$ its algebraic closure. The field $L = \bar{k}K$ is an infinite unramified abelian extension of K, which is not of interest to us.

When $D = 0$, the corresponding T-ray class field K_T^0 of K is the maximal unramified extension such that all places in T splits. We call K_T^0 the T-Hilbert class field of K, and denote it by $H_T(K)$. The Galois group of the extension $H_T(K)/K$ is the T-class group $Cl_T(K)$. Let ℓ be a prime, we will also consider the (T, ℓ)-Hilbert class field $K_{T,\ell}^0$ of K.

Definition 6.6. Let ℓ be a prime, the (T, ℓ)-Hilbert class field $K_{T,\ell}^0$ of K is the maximal unramified abelian ℓ-extension such that all places in T split. Its Galois group over K is the ℓ-part of the T-class group.

We end this section by stating a variant of the Hurwitz genus formula using the conductors. Let K/F be a geometric extension of function fields over $\mathbb{F}_q$ with an abelian Galois group G. A *Dirichlet character* of

K/F is a character of G, i.e. homomorphisms $\chi : G \to \mathbb{C}^*$. The fixed field of $\ker \chi$ is an abelian extension K_χ of F. We define the *Artin-conductor*, $\mathfrak{f}_\chi$ to be the conductor of K_χ. The genus of K can be expressed in terms of the genus of F and the conductors $\mathfrak{f}_\chi$.

Theorem 6.7 (Führerproduktdiskriminantformel)**.** *Let K/F be a geometric extension of function fields over $\mathbb{F}_q$ with an abelian Galois group G, then*

$$2g(K) - 2 = [K : F](2g(F) - 2) + \sum_\chi \deg \mathfrak{f}_\chi.$$

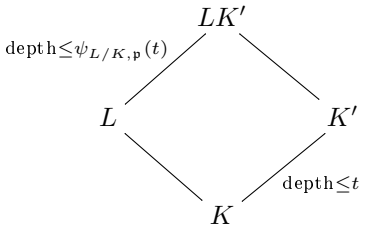
Here $\mathfrak{f}_\chi$ is the Artin-conductor of χ, and the sum runs through the characters χ of G.

Proof. See [93, Chap. 5]. □

6.2 Class field theory of wildly ramified extensions

We collect some lemmas on wildly ramified abelian extensions in this section. The first lemma concerns the behaviour of higher ramification groups under base change.

Lemma 6.8. *Let L/K be a Galois extension of global fields, and let K'/K be a Galois extension linearly disjoint from L. Let $\mathfrak{p}$ be a place of K, and let $\mathfrak{P}$, $\mathfrak{P}'$, $\mathfrak{p}'$ be compatible prolongations of $\mathfrak{p}$ to L, LK' and K' respectively. If K'/K is ramified of depth at most t at $\mathfrak{p}$, then LK'/L is ramified of depth at most $s = \psi_{L/K,\mathfrak{p}}(t)$ at $\mathfrak{P}$, where ψ is the inverse of ϕ defined in* (6.1).



Proof. The proof is by tracing the definitions of the ramification groups and using Lemma 6.3. □

Lemma 6.9. *Let L/K be an elementary abelian p-extension of global fields of characteristic p with Galois group G, and let $\mathfrak{p}$ be a place of K. Then the upper ramification jumps at $\mathfrak{p}$ are prime to p.*

Proof. The statement is well-defined by the Hasse-Arf theorem (see [74, p.76]). The lemma is then proved by induction on the number of jumps. When there is only one jump, then any degree p subfields of L/K have the same jump, and the lemma follows from Artin-Schreier theory (see [80, p. 115]). If there are n

jumps, let $G^{j_1} \supsetneq G^{j_2} \supsetneq \ldots \supsetneq G^{j_n} \supsetneq 1$ be the filtration by the upper ramification groups. Let L^n be the fixed field of G^{j_n}, then the upper ramification jumps of L^n/K are the first $n-1$ jumps of L/K. They are prime to p by induction hypothesis. As L/K is an elementary abelian p-extension, there is a degree p subextension L' such that $L = L^n L'$ and the only jump of L' is at j_n. Indeed if the jump of L' is of lower index than j_n, then $G^{j_n}(L^n/K) = G^{j_n}(L'/K) = 1$ which easily implies $G^{j_n} = 1$, a contradiction. If the jump of L' is of higher index, clearly we will see a higher ramification jump in L/K. Finally, the jump j_n is prime to p by Artin-Schreier theory. □

Lemma 6.10. *Let $M/L/K$ be a tower of Galois extensions of local fields, M/K abelian. Let $G = \mathrm{Gal}(M/K)$ and $H = \mathrm{Gal}(M/L)$. Let k be the residue field of K. Then for all i, the quotient of lower ramification groups H_i/H_{i+1} is a k-vector space of dimension at most one.*

Proof. This follows directly from Proposition 1 and 2 of [19]. □

Lemma 6.11. *Let L/K be a p-extension of global function fields of characteristic p, with constant field $\mathbb{F}_{p^e}$. Let $\mathfrak{P}$ be a place of L ramified in L/K and let $\mathfrak{p} = \mathfrak{P} \cap K$. Assume L/K is ramified of depth at most $\nu_\mathfrak{p}$ at $\mathfrak{p}$, and let $I_\mathfrak{p}$ be the inertia group at $\mathfrak{p}$. If $L_\mathfrak{P}/K_\mathfrak{p}$ is abelian, then*

$$d_p(I_\mathfrak{p}) \leq e \cdot \deg \mathfrak{p} \cdot (\nu_\mathfrak{p} - 1 - [(\nu_\mathfrak{p} - 1)/p]).$$

Proof. The lemma is local in nature, so we may localize and assume that our extension is abelian. Since the local extension is abelian and we are only interested in p-ranks, it suffices to prove the lemma when $I_\mathfrak{p}$ is elementary abelian. By the Hasse-Arf theorem, all jumps in the upper filtration are integers. By Lemma 6.9, the jumps are prime to p, and by Lemma 6.10, the p-rank is decreased by at most $e \cdot \deg \mathfrak{p}$ for each jump. The lemma now follows from a simple counting argument. □

We will also need the difference between the relation rank and the generator rank of the Galois group of an abelian p-extension and the generator rank of the ray class group.

Proposition 6.12. *Let L/K be an abelian p-extension of global function fields over $\mathbb{F}_q$ of characteristic p, and let $\mathfrak{p}$ be a place of degree $f_\mathfrak{p}$ in K. Assume that L/K is ramified of depth at most $\nu_\mathfrak{p}$. Then*

$$r_p(G_\mathfrak{p}) - d_p(G_\mathfrak{p}) \leq \binom{ef_\mathfrak{p}(\nu_\mathfrak{p} - 1) + 1}{2} = \frac{(ef_\mathfrak{p}(\nu_\mathfrak{p} - 1))(ef_\mathfrak{p}(\nu_\mathfrak{p} - 1) + 1)}{2}.$$

Here e is defined by $q = p^e$.

Proof. By Corollary 5.4, we have $r_p(G_\mathfrak{p}) - d_p(G_\mathfrak{p}) \leq r_p(I_\mathfrak{p})$. By Lemma 6.10, $I_\mathfrak{p}$ is a p-group of order at most $p^{e \cdot f_\mathfrak{p}(\nu_\mathfrak{p}-1)}$. Our $I_\mathfrak{p}$ is abelian since L/K is an abelian extension. Hence

$$r_p(I_\mathfrak{p}) \leq \binom{ef_\mathfrak{p}(\nu_\mathfrak{p}-1)+1}{2}$$

by Lemma 5.5. □

Proposition 6.13. *Let k be a function field and T be a set of non-empty rational places in k of size t. Let $\mathfrak{m} = \sum_\mathfrak{p} m_\mathfrak{p}\mathfrak{p}$ be a conductor whose support S is disjoint from T. The p-rank of the extension $k^T_\mathfrak{m}/k$ is at least*

$$d_p(\mathrm{Gal}(k^T_\mathfrak{m}/k)) \geq 1 + \sum_{\mathfrak{p}\in S} ef_\mathfrak{p} \cdot (\nu_\mathfrak{p} - 1 - [(\nu_\mathfrak{p}-1)/p]) - t.$$

Proof. For a singleton set T, the group contains the factor $\prod_{\mathfrak{p}\in S} U^{(1)}_\mathfrak{p}/U^{(\nu_\mathfrak{p})}_\mathfrak{p}$, which has p-rank

$$\sum_{\mathfrak{p}\in S} ef_\mathfrak{p} \cdot (\nu_\mathfrak{p} - 1 - [(\nu_\mathfrak{p}-1)/p])$$

by Lemma 4.2.5(i) of [66]. Now subtract $t-1$ for a set T of size t. □

6.3 Ramification of bounded depth

In this section we outline the theory of ramification of bounded depth. For details, see [36].

Let K be a global function field of characteristic p with constant field $\mathbb{F}_q$. Let S be a set of places in K, and $\nu : S \to [0,\infty]$ be a map sending $\mathfrak{p}$ to $\nu_\mathfrak{p}$. We extend ν to all places in K by setting $\nu_\mathfrak{p} = 0$ for all $\mathfrak{p} \notin S$.

Definition 6.14.

1. Let L/K be a Galois extension of global fields with Galois group G. We say that L/K has *ramification of depth at most n* at a place $\mathfrak{p}$ in K if the ramification groups $G^n_\mathfrak{P}$ in upper numbering are trivial for all places $\mathfrak{P}$ in L above $\mathfrak{p}$.

2. Let $\nu : S \to [0,\infty]$ be a map. We say that the *ramification depth of L/K is bounded by ν* if L/K has ramification of depth at most $\nu_\mathfrak{p}$ at any place $\mathfrak{p}$.

3. Define $K_{S,\nu}$ to be the maximal p-extension of K unramified outside S and with the property that the ramification depth of $K_{S,\nu}/K$ at $\mathfrak{p}$ is at most $\nu_\mathfrak{p}$ for any place $\mathfrak{p} \in S$. Let $G_{S,\nu} = \mathrm{Gal}(K_{S,\nu}/K)$. This is a p-group.

Suppose L/K is a finite Galois extension contained in $K_{S,\nu}$, and S_L is the set of all places in L lying above S. We lift the map ν in S to a map ν_L in S_L by setting

$$\nu_{L,\mathfrak{P}} = \psi_{L/K,\mathfrak{p}}(\nu_{\mathfrak{p}}), \tag{6.2}$$

where $\mathfrak{P} \in S_L$ is any place lying above $\mathfrak{p}$, and $\psi_{\mathfrak{P}/\mathfrak{p}}$ is given by the equation $G_{\mathfrak{P}}^s = G_{\psi_{\mathfrak{P}/\mathfrak{p}}(s),\mathfrak{P}}$ relating the upper and lower numberings of the ramification groups. This definition allows us to describe the extension $K_{S,\nu}/K$ as a tower of abelian extensions. Set $K_1 = K$, $S_1 = S$. We define K_{n+1} to be the maximal abelian extension of K_n contained in K_{S_n,ν_n}, and S_{n+1} the set of places in K_{n+1} lying above S_n, and ν_{n+1} the extension of ν from S_n to S_{n+1}. Let K_∞ be the union of all K_n.

Proposition 6.15. *Let K, S, ν be as above. Then $K_\infty = K_{S,\nu}$.*

Proof. See [36, Theorem 3.5]. □

Following the notations from [36], we set

$$\begin{aligned}
U_{\mathfrak{p}}^{(n)} &= \{x \in K_{\mathfrak{p}} | v_{\mathfrak{p}}(x-1) \geq n\} \text{ (the } n\text{-th higher unit group in } K_{\mathfrak{p}}), \\
\Delta &= \{x \in K^* | (x) \text{ is a } p\text{-th power in the group of fractional ideals of } K\}, \\
\Delta_S &= \{x \in \Delta | x \in K_{\mathfrak{p}}^{*p} \ \forall \mathfrak{p} \in S\}/K^{*p}, \\
\Delta_{S,\nu} &= \{x \in \Delta | x \in K_{\mathfrak{p}}^{*p} U_{\mathfrak{p}}^{(\nu_{\mathfrak{p}})} \ \forall \mathfrak{p} \in S\}/K^{*p}.
\end{aligned} \tag{6.3}$$

Then the generator rank $d_{S,\nu}$ of $G_{S,\nu}$ is given by the following proposition.

Proposition 6.16.

$$d_{S,\nu} = 1 + d_p(\Delta_{S,\nu}) + \sum_{\mathfrak{p} \in S} d_p\left(\frac{U_{\mathfrak{p}}^{(1)}}{U_{\mathfrak{p}}^{(\nu_{\mathfrak{p}})}}\right).$$

Proof. This proposition is the function field analogue of [36, Theorem 3.7], and the proof follows the same line as in that theorem. We outline the proof here. Let I_K be the group of ideles of K, and let $\mathcal{U}_{S,\nu} = \prod_{\mathfrak{p} \notin S} U_{\mathfrak{p}} \prod_{\mathfrak{p} \in S} U_{\mathfrak{p}}^{(\nu_{\mathfrak{p}})}$. In particular, if $S = \varnothing$, we write $\mathcal{U}_\varnothing = \prod_{\mathfrak{p}} U_{\mathfrak{p}}$. Consider the following exact sequence

$$1 \to \Delta_{S,\nu} \to \Delta/K^{*p} \to \frac{\mathcal{U}_\varnothing}{\mathcal{U}_\varnothing^p \mathcal{U}_{S,\nu}} \to \frac{I_K}{\mathcal{U}_{S,\nu} I_K^p} \to \frac{I_K}{K^* \mathcal{U}_\varnothing I_K^p} \to 1$$

in class field theory. Note that $\frac{I_K}{K^* \mathcal{U}_\varnothing I_K^p} = \frac{Cl_K}{Cl_K^p}$, and $d_p(\Delta_\varnothing) = d_p(Cl_K)$ since $d_p(\mathbb{F}_q^*) = 0$. Let $\mathfrak{m} = \sum_{\mathfrak{p} \in S} \nu_{\mathfrak{p}} \mathfrak{p}$ be the conductor corresponding to ν. Taking account of the constant fields in $K_{S,\nu}$ and Cl_K, we obtain $d_p(G_{S,\nu}) = d_p(Cl^{\mathfrak{m}}(K)) + 1$. Putting all these together gives the proposition. □

To calculate the generator rank above, we need the following.

Proposition 6.17. *Let K be a global function field of characteristic p, with full constant field $\mathbb{F}_q$, where $q = p^e$. Let $\mathfrak{p}$ be a place in K of degree f, then*

$$d_p\left(\frac{U_{\mathfrak{p}}^{(1)}}{U_{\mathfrak{p}}^{(\nu_{\mathfrak{p}})}}\right) = f \cdot e \cdot (\nu_{\mathfrak{p}} - 1 - [(\nu_{\mathfrak{p}} - 1)/p]),$$

where $[\cdot]$ denotes the integer part.

Proof. This is [66, Lemma 4.2.5 (i)]. □

Combining Proposition 6.16 and 6.17, we get the following theorem.

Theorem 6.18. *Let K be a global function field of characteristic p, with full constant field $\mathbb{F}_q$, where $q = p^e$. For a place $\mathfrak{p}$ in K let $f_{\mathfrak{p}}$ be its degree. The generator rank $d_{S,\nu}$ of $G_{S,\nu} = \mathrm{Gal}(K_{S,\nu}/K)$ satisfies*

$$d_{S,\nu} = 1 + d_p\Delta_{S,\nu} + \sum_{\mathfrak{p}\in S} e f_{\mathfrak{p}}(\nu_{\mathfrak{p}} - 1 - [(\nu_{\mathfrak{p}} - 1)/p]).$$

Chapter 7

Group extensions and the embedding problem

We will be constructing class field towers by solving the embedding problems. This requires the knowledge of group extensions and unramified cohomology. We summarize the necessary backgrounds here.

7.1 Group extensions

Let G and N be groups. A *group extension* of G by N is a short exact sequence

$$\epsilon : 1 \longrightarrow N \longrightarrow E \xrightarrow{j} G \longrightarrow 1$$

By abuse of language, sometimes we will say E is the group extension of G by N. The extension ϵ is *split* if this sequence admits a section, i.e. there is a homomorphism $s : G \to E$ such that $j \circ s = \mathrm{id}_G$. Two extensions $\epsilon_i : 1 \to N \to E_i \to G \to 1$, $1 = 1, 2$, are said to be *equivalent* if there is an isomorphism $\phi : E_1 \to E_2$ so that the diagram

$$\begin{array}{ccccccccc} \epsilon_1 : 1 & \longrightarrow & N & \longrightarrow & E_1 & \longrightarrow & G & \longrightarrow & 1 \\ & & \| & & \downarrow{\scriptstyle \phi} & & \| & & \\ \epsilon_2 : 1 & \longrightarrow & N & \longrightarrow & E_2 & \longrightarrow & G & \longrightarrow & 1 \end{array}$$

commutes.

From now on we restrict our attention to the case when N is an abelian group, and we write A in place of N.

$$\epsilon : 0 \longrightarrow A \xrightarrow{i} E \xrightarrow{j} G \longrightarrow 1$$

In this case G has an action on A which makes A a G-module: A can be embedded as a normal subgroup of E via i, so E acts on A by conjugation. This action of A by conjugation on itself is trivial since A is abelian. So we get an induced action of $E/A \cong G$ on A. Note that $i(A)$ is central in E (i.e. $i(A)$ lies inside the center of E) if and only if the G-action on A is trivial. This action allows us to classify all central extensions of G

by A using group cohomology.

Proposition 7.1. *There is a bijection between the set of equivalence classes of central group extensions, denoted by $E(G, A)$, of a group G by an abelian group A and the cohomology group $H^2(G, A)$.*

Proof. See [92, Sec. 6.6]. □

Definition 7.2. Let E_1, E_2, G be groups, $j_1 : E_1 \to G$ and $j_2 : E_2 \to G$ be two homomorphisms. The *pullback* of E_1 and E_2 over G, denoted by $E_1 \times_G E_2$, is defined by

$$E_1 \times_G E_2 := \{(e_1, e_2) \in E_1 \times E_2 | j_1(e_1) = j_2(e_2) \text{ in } G\}.$$

The group operation of $E_1 \times_G E_2$ is the one induced from the direct product $E_1 \times E_2$.

We know that $H^2(G, A)$ is an abelian group. There is also a group structure on $E(G, A)$, called the *Baer sum*, defined as follows. Let

$$\epsilon_1 : 0 \longrightarrow A \xrightarrow{i_1} E_1 \xrightarrow{j_1} G \longrightarrow 1$$
$$\epsilon_2 : 0 \longrightarrow A \xrightarrow{i_1} E_2 \xrightarrow{j_2} G \longrightarrow 1$$

be two extensions. Let E_3 be the pullback $E_1 \times_G E_2$. It is easy to see that there are two copies of A inside E_3, namely $A \times \{0\}$ and $\{0\} \times A$. There is also the skew-diagonal copy $\{(-a, a) | a \in A\}$. If we take the quotient E of E_3 by the skew-diagonal, the two copies $A \times \{0\}$ and $\{0\} \times A$ are identified. It is not difficult to see that

$$\epsilon : 0 \longrightarrow A \xrightarrow{i} E \xrightarrow{j} G \longrightarrow 1$$

is an extension, where i and j are the maps induced from i_1 and j_1 (or from i_2 and j_2, which yields the same maps as that from i_1 and j_1). The class of ϵ is by definition the Baer sum of the classes ϵ_1 and ϵ_2. It can be shown that the Baer sum is well-defined, commutative, and corresponds to the sum in $H^2(G, A)$ via the bijection in Proposition 7.1 (see [92, Sec. 3.4, 6.6]). We will not need the sums in this thesis.

7.2 Unramified cohomology

In this section we describe the necessary background on unramified cohomology. For details, see [60, 76].

Definition 7.3. Let L/K be a Galois extension of global function fields with Galois group G. For a place

$\mathfrak{p}$ in K, and a G-module A, define

$$H^i_{nr}(G_\mathfrak{p}, A) = \mathrm{im}(H^i(G_\mathfrak{p}/I_\mathfrak{p}, A^{I_\mathfrak{p}}) \xrightarrow{inf} H^i(G_\mathfrak{p}, A)),$$

where inf is the inflation map.

We are interested in the unramified cohomology $H^2_{nr}(G_\mathfrak{p}, \mathbb{Z}/p\mathbb{Z})$ since they will characterize the extensions we need later. If L/K is a p-extension, and $\mathfrak{p}$ is unramified in L/K, then

$$H^2_{nr}(G_\mathfrak{p}, \mathbb{Z}/p\mathbb{Z}) = H^2(G_\mathfrak{p}, \mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$$

if $G_\mathfrak{p} \neq 1$. Let L/K be a p-extension of global fields with Galois group G unramified outside a set S of places of K. Define $S_{nr} = \{\mathfrak{p} \in S | d_p(I_\mathfrak{p} G'_\mathfrak{p}/G'_\mathfrak{p}) = d_p(G_\mathfrak{p}) - 1\}$, where G' is the commutator subgroup of G.

Remark 7.4. Suppose L/K is as above, and $\mathfrak{p}$ is a place in S. Let $L^{ab}_\mathfrak{p}/K_\mathfrak{p}$ be the maximal abelian subextension of $L_\mathfrak{p}/K_\mathfrak{p}$. Then the set S_{nr} consists of exactly those places in S such that $d_p(G_\mathfrak{p}) = d_p(G^{ab}_\mathfrak{p}) = d_p(I^{ab}_\mathfrak{p}) + 1$. The other places $\mathfrak{p} \in S \backslash S_{nr}$ satisfy $d_p(G_\mathfrak{p}) = d_p(I^{ab}_\mathfrak{p})$.

If $\mathfrak{p}$ is ramified, the unramified cohomology is given by the following proposition.

Proposition 7.5. *Let L/K be a p-extension with Galois group G unramified outside a set S of places in K. Let $\mathfrak{p} \in S$, then*

$$H^2_{nr}(G_\mathfrak{p}, \mathbb{Z}/p\mathbb{Z}) = \begin{cases} \mathbb{Z}/p\mathbb{Z} & , \mathfrak{p} \in S_{nr}, \\ 0 & , \text{ otherwise.} \end{cases}$$

Proof. Define f by $G_\mathfrak{p}/I_\mathfrak{p} \cong \mathbb{Z}/p^f\mathbb{Z}$. From the exact sequence

$$1 \to I_\mathfrak{p} \to G_\mathfrak{p} \to G_\mathfrak{p}/I_\mathfrak{p} \to 1,$$

we obtain by the Lyndon-Hochschild-Serre spectral sequence (see for example [92]) the following exact sequence.

$$0 \longrightarrow H^1(G_\mathfrak{p}/I_\mathfrak{p}, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{inf} H^1(G_\mathfrak{p}, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{res_1} H^1(I_\mathfrak{p}, \mathbb{Z}/p\mathbb{Z})^{G_\mathfrak{p}/I_\mathfrak{p}}$$

$$\longrightarrow H^2(G_\mathfrak{p}/I_\mathfrak{p}, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{inf_2} H^2(G_\mathfrak{p}, \mathbb{Z}/p\mathbb{Z}).$$

Since $H^2(\mathbb{Z}/p^f\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$, we have $H^2_{nr}(G_\mathfrak{p}, \mathbb{Z}/p\mathbb{Z}) \cong \mathbb{Z}/p\mathbb{Z}$ if and only if inf_2 is injective, and $H^2_{nr}(G_\mathfrak{p}, \mathbb{Z}/p\mathbb{Z}) = 0$ otherwise. By exactness, inf_2 is injective if and only if res_1 is surjective. Looking at

the p-ranks we see that this is equivalent to $d_p(H^1(I_\mathfrak{p}, \mathbb{Z}/p\mathbb{Z})) = d_\mathfrak{p}(G_\mathfrak{p}) - 1$. By a little computation we see that $d_p(H^1(I_\mathfrak{p}, \mathbb{Z}/p\mathbb{Z})) = d_p(I_\mathfrak{p}G'_\mathfrak{p}/G'_\mathfrak{p})$. This finishes the proof of the proposition. □

7.3 The embedding problem

The embedding problem is the induction step in the construction of field extensions with prescribed Galois group. In this section, we outline some parts of the theory and omit most details, which the readers may find in [58, 60].

Definition 7.6. Let $\mathfrak{G}$ be a profinite group. An *embedding problem* $\mathcal{E}(\mathfrak{G})$ is a diagram

$$\begin{array}{ccccccccc} & & & & & & \mathfrak{G} & & \\ & & & & & & \downarrow{\scriptstyle \phi} & & \\ \epsilon: 0 & \longrightarrow & A & \longrightarrow & E & \xrightarrow{j} & G & \longrightarrow & 1 \end{array}$$

where A, E, G are finite groups, A is abelian, ϵ is a short exact sequence and ϕ is surjective. A solution to the problem is a continuous homomorphism $\chi : \mathfrak{G} \to E$ making the above diagram commutative.

$$\begin{array}{ccccccccc} & & & & & & \mathfrak{G} & & \\ & & & & & \overset{\chi}{\swarrow} & \downarrow{\scriptstyle \phi} & & \\ \epsilon: 0 & \longrightarrow & A & \longrightarrow & E & \xrightarrow{j} & G & \longrightarrow & 1 \end{array}$$

The solution χ is called proper if it is surjective. The group A is called the *kernel* of the embedding problem $\mathcal{E}(\mathfrak{G})$.

The following proposition is useful to determine if an embedding problem has a solution. Let $inf^G_\mathfrak{G} : H^2(G, A) \to H^2(\mathfrak{G}, A)$ be the inflation map induced from $\phi : \mathfrak{G} \to G$.

Proposition 7.7 (Hoechsmann [44])**.** *The embedding problem $\mathcal{E}(\mathfrak{G})$ has a solution if and only if $inf^G_\mathfrak{G}(\epsilon) = 1$.*

Proof. See [60, Prop. 3.5.9]. □

Now let $\mathfrak{G}_K$ be the absolute Galois group of K, L/K be a finite Galois extension, and $G = \mathrm{Gal}(L/K)$ be its Galois group. Let S be a set of places in K and S_L the set of places in L lying above S. The global embedding problem $(L/K, \epsilon, S_L)$ is defined as follows.

Definition 7.8. Let L/K be a finite extension, and $G = \mathrm{Gal}(L/K)$ its Galois group. Let

$$\epsilon: 0 \longrightarrow A \longrightarrow E \xrightarrow{j} G \longrightarrow 1$$

be an exact sequence, where A, E are finite groups with A abelian. A *global embedding problem* $(L/K, \epsilon, S_L)$ is a diagram

$$\begin{array}{ccccccccc} & & & & & & \mathfrak{G}_K & & \\ & & & & & & \downarrow \phi & & \\ \epsilon: 0 & \longrightarrow & A & \longrightarrow & E & \xrightarrow{j} & G & \longrightarrow & 1 \end{array}$$

where ϕ is the restriction map.

A *solution* of the embedding problem is a continuous homomorphism $\chi : \mathfrak{G}_K \to E$ making the diagram

$$\begin{array}{ccccccccc} & & & & & & \mathfrak{G}_K & & \\ & & & & & \overset{\chi}{\swarrow} & \downarrow \phi & & \\ \epsilon: 0 & \longrightarrow & A & \longrightarrow & E & \xrightarrow{j} & G & \longrightarrow & 1 \end{array}$$

commutative, and such that M/L is unramified outside S_L, where M is the fixed field of the kernel of χ. The solution χ is called *proper* if it is surjective.

Note that in the above setting, a proper solution of the embedding problem $(L/K, \epsilon, S_L)$ corresponds to a Galois extension M/K, with $\mathrm{Gal}(M/L) = A$ and is unramified outside S_L. By abuse of notation we also say that M is a solution of $(L/K, \epsilon, S_L)$. One important fact we need is that if L/K is a p-extension, the embedding problem with kernel $\mathbb{Z}/p\mathbb{Z}$ is solvable. More precisely, we have the following.

Proposition 7.9. *Let L/K be a Galois p-extension, and let S_L be a finite, non-empty set of places in L containing the ramified places of L/K. Let*

$$\epsilon: 0 \longrightarrow \mathbb{Z}/p\mathbb{Z} \longrightarrow E \longrightarrow G(L/K) \longrightarrow 1$$

be a non-split extension (meaning that ϵ is a non-split exact sequence). If $S_L \cap K = S_K$, then the global embedding problem $(L/K, \epsilon, S_L)$ has a proper solution M with the same constant field as L.

Proof. Let $\mathfrak{G}_{S_{K,p}}$ be the Galois group of the maximal pro-p-extension of K unramified outside S_K. Then we have the diagram

$$\begin{array}{ccccccccc} & & & & & & \mathfrak{G}_{S_{K,p}} & & \\ & & & & & \overset{\chi}{\swarrow} & \downarrow \phi & & \\ \epsilon: 0 & \longrightarrow & \mathbb{Z}/p\mathbb{Z} & \longrightarrow & E & \xrightarrow{j} & G(L/K) & \longrightarrow & 1 \end{array}$$

where ϕ is the restriction map. Since $H^2(\mathfrak{G}_{S_{K,p}}, \mathbb{Z}/p\mathbb{Z})$ is trivial (see [60, Cor. 8.3.2]), we must have $inf^{G(L/K)}_{\mathfrak{G}_{S_{K,p}}}(\epsilon) = 1$. The proposition now follows from Proposition 7.7. □

7.3.1 Independence of solutions to the global embedding problems

Let L/K be a Galois p-extension with Galois group $G = \mathrm{Gal}(L/K)$. Fix a finite, non-empty set S_L of places in L containing the ramified places of L/K. For each $\epsilon \in H^2(G, \mathbb{Z}/p\mathbb{Z})$, the corresponding global embedding problem $(L/K, \epsilon, S_L)$ has a proper solution by Proposition 7.9. The main result in this section is the following.

Proposition 7.10. *Let $\epsilon_1, \ldots, \epsilon_n$ be n linearly independent elements in $H^2(G, \mathbb{Z}/p\mathbb{Z})$, and let $M_1, \ldots, M_n$ are proper solutions to the global embedding problems corresponding to ϵ_i respectively. Let $M = M_1 \ldots M_n$ be the compositum of the solutions. Then $d_p(\mathrm{Gal}(M/L)) = n$.*

To prove Proposition 7.10, we start with some observations.

Lemma 7.11. *Let G be a group, and let $A_1, \ldots, A_n$ be abelian groups. For each $1 \leq i \leq n$, let $\epsilon_i \in H^2(G, A_i)$ be elements corresponding to the extensions*

$$\epsilon_i : 0 \longrightarrow A_i \longrightarrow E_i \longrightarrow G \longrightarrow 1$$

under Proposition 7.1. Then the element $(\epsilon_1, \ldots, \epsilon_n) \in H^2(G, \oplus_{i=1}^n A_i) = \oplus_{i=1}^n H^2(G, A_i)$ corresponds to the extension

$$\epsilon_i : 0 \longrightarrow \oplus_{i=1}^n A_i \longrightarrow E_1 \times_G E_2 \times_G \ldots \times_G E_n \longrightarrow G \longrightarrow 1.$$

Proof. For $n = 2$ the lemma follows from a detailed tracing of the bijection in Proposition 7.1. The case for general n then follows from induction. □

Lemma 7.12. *Let L, K, S_L and G be as in the first paragraph of this subsection. Suppose $\epsilon_1, \ldots, \epsilon_n \in H^2(G, \mathbb{Z}/p\mathbb{Z})$, and $M_1, \ldots, M_n$ be solutions to the global embedding problems $(L/K, \epsilon_i, S_L)$. If we have $M_i \cap \prod_{j \neq i} M_j = L$ for all i, then M is a solution to the global embedding problem $(L/K, (\epsilon_1, \ldots, \epsilon_n), S_L)$.*

Proof. If $M_i \cap \prod_{j \neq i} M_j = L$ for all i, then we know from Galois theory that

$$\mathrm{Gal}(M/K) = \mathrm{Gal}(M_1/K) \times_G \ldots \times_G \mathrm{Gal}(M_n/K).$$

The lemma now follows from Lemma 7.11 directly. □

Proof of Proposition 7.10. Let $\tilde{M}_i = M_1 M_2 \ldots M_i$, thus $M = \tilde{M}_n$. Clearly $d_p(\mathrm{Gal}(M/L)) \leq n$. Suppose that $d_p(\mathrm{Gal}(M/K)) < n$. Let j be the smallest integer j such that

$$d_p(\mathrm{Gal}(\tilde{M}_j)/L) = d_p(\mathrm{Gal}(\tilde{M}_{j+1})/L) = j. \tag{7.1}$$

In this case we have $M_{j+1} \subseteq \tilde{M}_j$ since each $\mathrm{Gal}(M_i/L) \cong \mathbb{Z}/p\mathbb{Z}$. The extensions M_i/L are Galois of degree p, so they are Artin-Schreier extensions [51, Theorem VI.6.4]. Hence $\mathrm{Gal}(\tilde{M}_j/L) \cong (\mathbb{Z}/p\mathbb{Z})^j$. The degree p subfields of $\tilde{M}_j$ are the fixed fields of the kernels of the non-trivial homomorphisms $(\mathbb{Z}/p\mathbb{Z})^j \to \mathbb{Z}/p\mathbb{Z}$, which are linear maps. These maps induce linear maps $H^2(G, (\mathbb{Z}/p\mathbb{Z})^j) \to H^2(G, \mathbb{Z}/p\mathbb{Z})$ on the cohomology groups. In particular, for the homomorphism $\phi : \mathrm{Gal}(\tilde{M}_j/L) \to \mathrm{Gal}(M_{j+1}/L)$ that realize the extensions $\tilde{M}_j/M_{j+1}/L$, it is not difficult to show that ϕ corresponds to the map of extensions

$$\begin{array}{ccccccccc}
\epsilon : 1 & \longrightarrow & \mathrm{Gal}(\tilde{M}_j/L) & \longrightarrow & \mathrm{Gal}(\tilde{M}_j/K) & \longrightarrow & G & \longrightarrow & 1 \\
 & & \downarrow{\scriptstyle \phi} & & \downarrow{\scriptstyle \tilde{\phi}} & & \| & & \\
\phi^*\epsilon : 1 & \longrightarrow & \mathrm{Gal}(M_{j+1}/L) & \longrightarrow & \mathrm{Gal}(M_{j+1}/K) & \longrightarrow & G & \longrightarrow & 1.
\end{array}$$

By (7.1), the fields $M_1, \ldots, M_j$ satisfy $M_i \cap \prod_{l \neq i} M_l = L$ for all i. Therefore, $\tilde{M}_j$ corresponds to the element $\epsilon = (\epsilon_1, \ldots, \epsilon_j)$ by Lemma 7.12, and the p subextension M_{j+1} of $\tilde{M}_j$ corresponds to $\phi^*(\epsilon)$, which is a linear combination of $\epsilon_1, \ldots, \epsilon_j$ as ϕ is linear. On the other hand, we know that the p-extension M_{j+1} corresponds to ϵ_{j+1}. Thus ϵ_{j+1} is a linear combination of $\epsilon_1, \ldots, \epsilon_j$. This is a contradiction. $\square$

Chapter 8

Asymptotic towers of function fields

8.1 The Ihara constant

In Chapter 3, we have seen that the Weil upper bound is not sharp when the genus of a function field becomes large compare to the number of elements over the ground field. In particular, Theorem 3.3 tells us that a function field $K/\mathbb{F}_q$ can only attain the Weil upper bound when its genus $g(K) \leq \sqrt{q}(\sqrt{q}-1)/2$. Therefore, it is of interest to understand the asymptotic upper bound of the number of rational places of a function field K compared to its genus as the genus goes to infinity, when the number of elements in the ground field is fixed. A measure of such asymptotic behaviour is the Ihara constant.

Definition 8.1. For a function field K over $\mathbb{F}_q$, denote $N(K)$ its number of rational places. Put

$$N_q(g) := \max N(K),$$

where the maximum is taken over all function fields $K/\mathbb{F}_q$ with genus g. The *Ihara constant* $A(q)$ is defined by

$$A(q) := \limsup_{g\to\infty} \frac{N_g(q)}{g}.$$

From the Weil bound, one easily gets $A(q) \leq 2\sqrt{q}$, and Serre's bound (Theorem 3.2) shows that $A(q) \leq [2\sqrt{q}]$. The best upper bound is obtained by Drinfel′d and Vlăduţ [15]. The following proof is reproduced from Stichtenoth [80], using Serre's explicit formulas (Proposition 3.4).

Theorem 8.2 (Drinfel′d-Vlăduţ)**.** $A(q) \leq \sqrt{q} - 1$.

Proof. Notations and setting as in Proposition 3.4. Let

$$c_r = 1 - \frac{r}{m}, \qquad r = 1, \ldots, m.$$

Then

$$\lambda_m(t) = \sum_{r=1}^{m} \left(q - \frac{r}{m}\right) t^r.$$

We need to verify the two properties in Proposition 3.4. The first property is evident. For the second property, the case for $t = 1$ is clear. For $t \neq 1$, consider the function

$$u(t) = \sum_{r=1}^{m} t^r = \frac{t^{m+1} - t}{t - 1}.$$

Thus $u'(t) = \sum_{r=1}^{m} r t^{r-1}$, and hence

$$\frac{tu'(t)}{m} = \sum_{r=1}^{m} \frac{r}{m} t^r,$$

and

$$\begin{aligned} \lambda_m(t) = \sum_{r=1}^{m} \left(q - \frac{r}{m}\right) t^r &= u(t) - \frac{tu'(t)}{m} \\ &= \frac{t}{(t-1)^2} \left(\frac{t^m - 1}{m} + 1 - t\right). \end{aligned}$$

Therefore,

$$f_m(t) = 1 + \lambda_m(t) + \lambda_m(t^{-1}) = \frac{2 - (t^m + t^{-m})}{m(t-1)(t^{-1} - 1)} = \frac{2 - 2\mathrm{Re}(t^m)}{m\,|t-1|^2},$$

which is positive (since $t \neq 1$). Proposition 3.4 then gives the upper bound

$$\frac{N}{g} \leq \frac{1}{\lambda_m(q^{-1/2})} + \frac{1}{g}\left(1 + \frac{\lambda_m(q^{1/2})}{\lambda_m(q^{-1/2})}\right), \tag{8.1}$$

where N is the number of rational places of an arbitrary function field over $\mathbb{F}_q$ of genus g. As m, g tends to infinity, the right hand side of (8.1) tends to $q^{1/2} - 1$. This finishes the proof. □

When q is a square, Ihara [46] and Tsfasman-Vlăduţ-Zink [86] independently showed that the Drinfel′d-Vlăduţ upper bound $A(q) = \sqrt{q} - 1$ can be achieved. Later, Garcia and Stichtenoth [23] went a step further by giving an explicit recursive tower that attains the Drinfel′d-Vlăduţ bound when q is a square. This allows a lot of applications to coding theory where explicit construction of the towers are needed, for example the explicit construction of asymptotically good families of linear codes that beat the asymptotic Gilbert-Varshamov bound [86].

However, we know much less when q is not a square. Many lower bounds are obtained for $A(q)$, but most of them are rather weak. Serre proved that $A(q) \geq c \log q$ for some absolute constant c by the class field tower method (see [75] and [10, Chapter IX]), and Temkine [84], using the same method, improved this to

$A(q^n) = (c' n \log q)^2/(\log n + \log q)$ with c' an effectively computable constant. Variations of Serre's result were also obtained in [65] and [57]. When $q = p^3$ is a cube of a prime, Zink [102] obtained the lower bound

$$A(p^3) \geq \frac{2(p^2-1)}{p+2}$$

using the idea of degenerated Shimura surfaces. His result was generalized to a general prime power q by Bezerra-Garcia-Stichtenoth [6] (see also [5] and for the case $q = 8$, [89]). Very recently, using the recursive tower method, Garcia-Stichtenoth-Bassa-Beelen [25] improve substantially the lower bounds for $A(p^n)$ when p is a prime and $n \geq 3$ is odd. Their lower bound is the following.

Proposition 8.3. *Let p be a prime and $n = 2m+1 \geq 3$ is odd. Then*

$$A(p^n) \geq \frac{2(p^{m+1}-1)}{p+1+\epsilon} \text{ with } \epsilon = \frac{p-1}{p^m-1}.$$

However, the recursive tower method is not successful over prime fields. There are even evidences that a good recursive tower over $\mathbb{F}_p$ may not exist [54].

When p is a small prime, some good lower bounds for $A(p)$ are also obtained using variations of Serre's class field tower method. Lower bounds for $A(2)$ appear in [75], [72], [64], [95], and lower bounds for $A(3)$ in [64], [84]. Lower bounds for $A(3)$ using tamely ramified towers appear in [3], [35, Section 4.2]. Among these results, the best lower bounds are the following.

Proposition 8.4 (Xing-Yeo [95] for $A(2)$, Aitken-Hajir [35] for $A(3)$)**.**

$$A(2) \geq \frac{97}{376} = 0.257979\ldots$$
$$A(3) \geq \frac{12}{25} = 0.48.$$

In [49], Kuhnt obtained a better lower bound for $A(2)$.

Proposition 8.5 (Kuhnt [49])**.**

$$A(2) \geq \frac{39}{129} = 0.302325\ldots.$$

For a survey about the recent developments on upper and lower bounds for $A(q)$, see [56]. We will improve the lower bounds for $A(2)$ and $A(3)$ further in the next chapter (see Theorem 9.3 and Theorem 9.4). Our method is based on the Serre's class field tower method. Before we go into the details of the class field tower method, we will review some properties about towers in the next section.

8.2 Asymptotic behaviour of towers

One conventional way to obtain lower bounds for $A(q)$ is by constructing towers of function fields. We will follow the book [66, Chap. 5].

Definition 8.6. A *tower of function fields* over $\mathbb{F}_q$ is a chain of function fields

$$\mathcal{F} = (F_1 \subsetneq F_2 \subsetneq \ldots)$$

over $\mathbb{F}_q$ with the following properties:

1. For each $i \geq 1$, the extension F_{i+1}/F_i is separable.
2. $g(F_j) > 1$ for some $j \geq 1$.

Note that the second condition and the Hurwitz genus formula imply that $g(F_i) \to \infty$.

If $\mathcal{F} = (F_1 \subsetneq F_2 \subsetneq \ldots)$ and $\mathcal{E} = (E_1 \subsetneq E_2 \subsetneq \ldots)$ be two towers over $\mathbb{F}_q$, the tower $\mathcal{E}$ is said to be a *subtower* of $\mathcal{F}$ if there is an embedding

$$\cup_{i\geq 1} E_i \hookrightarrow \cup_{i \geq 1} F_i.$$

That is, for any $i \geq 1$, there is an index $m = m(i) \geq 1$ such that $E_i \subseteq F_m$.

Proposition 8.7. *For any tower $\mathcal{F} = (F_1 \subsetneq F_2 \subsetneq \ldots)$, the sequence $\{N(F_i)/g(F_i)\}_{i\geq 1}$ is convergent.*

Proof. First we claim that if E/F is a finite extension of function fields over $\mathbb{F}_q$ with $g(F) > 1$, then

$$\frac{N(E)}{g(E)-1} \leq \frac{N(F)}{g(F)-1}.$$

To see this, we can assume that E/F is separable, for we have a subextension $E/E'/F$ with E/E' purely inseparable and E'/F separable. However, since E/E' is a purely inseparable extension, we have $N(E) = N(E')$ and $g(E) = g(E')$. With this assumption, we have by the Hurwitz genus formula,

$$\begin{aligned} g(E) - 1 &= [E:F](g(F)-1) + \frac{1}{2}\deg \mathrm{Diff}(E/F) \\ &\geq [E:F](g(F)-1). \end{aligned}$$

On the other hand, it is easy to see that $N(E) \leq [E:F]N(F)$. So

$$\frac{N(E)}{g(E)-1} \leq \frac{[E:F]N(F)}{[E:F](g(F)-1)} = \frac{N(F)}{g(F)-1}.$$

Back to the proof of the proposition, we may assume that $g(F_i) > 1$ for all i. The sequence $\{N(F_i)/(g(F_i)-1)\}_{i\geq 1}$ is non-increasing and bounded below by zero, hence it is convergent. Since $g(F_i) \to \infty$, the sequence $\{N(F_i)/(g(F_i))\}_{i\geq 1}$ is also convergent and has the same limit. □

Definition 8.8. Let $\mathcal{F} = (F_1 \subsetneq F_2 \subsetneq \ldots)$ be a tower over $\mathbb{F}_q$. The quantity

$$\lambda(\mathcal{F}) = \lim_{i\to\infty} \frac{N(F_i)}{g(F_i)}$$

is called the *limit* of the tower $\mathcal{F}$. It is obvious that $\lambda(\mathcal{F}) \leq A(q)$.

The tower $\mathcal{F}$ is said to be *asymptotically good* (respectively *asymptotically bad*) if $\lambda(\mathcal{F}) > 0$ (respectively $\lambda(\mathcal{F}) = 0$), and is *asymptotically optimal* if $\lambda(\mathcal{F}) = A(q)$.

Corollary 8.9. *If $\mathcal{E}$ and $\mathcal{F}$ are two towers over $\mathbb{F}_q$, with $\mathcal{E}$ being a subtower of $\mathcal{F}$. Then*

1. *$\lambda(\mathcal{E}) \geq \lambda(\mathcal{F})$.*
2. *If $\mathcal{E}$ is asymptotically bad, then $\mathcal{F}$ is also asymptotically bad.*
3. *If $\mathcal{F}$ is optimal, then $\mathcal{E}$ is also optimal.*

Proof. This follows easily from Proposition 8.7. □

Remark 8.10. It is in general difficult to find asymptotically good towers of function fields. There are many conditions to guarantee a tower to be asymptotically good (or bad). An example is that if $\mathcal{F}$ is an abelian tower (meaning that all extensions F_i/F_1 are abelian), then the tower is asymptotically bad (see [19]. In this thesis, we will only be interested in unramified towers, for which conditions for asymptotically good (or bad) towers are easier to handle.

8.3 Serre's class field tower method

To apply the class field tower method, we first fix a field $K/\mathbb{F}_q$ of genus g, called the *ground field*. Let ℓ be a prime and T be a non-empty set of rational places in K. We construct the (T,ℓ)-class field tower as follows: Let $K_0 = K$, $T_0 = T$. For each $i > 0$, set K_i to be the (T_{i-1},ℓ)-Hilbert class field of K_{i-1} and T_i be the set of places in K_i lying over the places in T_{i-1}. We thus obtain a tower

$$K \subseteq K_1 \subseteq K_2 \subseteq \ldots \subseteq K_i \subseteq \ldots,$$

which is the (T,ℓ)-*Hilbert class field tower* over K. If the tower is infinite, then we can get a lower bound for $A(q)$.

Proposition 8.11. *Let ℓ be a prime, $K/\mathbb{F}_q$ be a function field of genus $g > 1$, and let T be a non-empty set of rational places in K. If K has an infinite (T,ℓ)-Hilbert class field tower, then*

$$A(q) \geq \frac{|T|}{g-1}.$$

Proof. Let K_i and T_i be as in the paragraph prior to this proposition. The tower is infinite, so $\lim_{i\to\infty}[K_i : K] = \infty$. Let $N_i = N(K_i)$ be the number of rational places of K_i, and let $g_i = g(K_i)$ be its genus. By the Hurwitz genus formula,

$$2g_i - 2 = [K_i : K](2g-2)$$

since K_i/K is a separable unramified extension. For the N_i we have

$$N_i \geq |T_i| = [K_i : K]\,|T|$$

since all places in T split completely in K_i/K.

From the definition of $A(q)$, we have

$$A(q) \geq \limsup_{i\to\infty} \frac{N_i}{g_i} \geq \lim_{i\to\infty} \frac{[K_i : K]\,|T|}{[K_i : K](g-1)+1} = \frac{|T|}{g-1}.$$

This completes the proof. □

With the above proposition, to get lower bounds for $A(q)$, it remains to determine conditions to guarantee that a (T,ℓ)-Hilbert class field tower over K is infinite. Let $L = \cup_{i=0}^{\infty} K_i$ be the union of the K_i, and let G be the Galois group of L/K. Clearly G is an pro-ℓ-group. We first show that L/K is Galois.

Proposition 8.12. *The tower $L = \cup_{i=0}^{\infty} K_i$ is Galois over K.*

Proof. We show that K_i/K are Galois for all $i \geq 1$ by induction. The case $i = 1$ is well-known. Assume that K_i/K is Galois for some i, then as both K_i/K and K_{i+1}/K_i are separable, so is the extension K_{i+1}/K. Fix an algebraic closure $\bar{K}$ of K containing K_{i+1}, and let $\sigma : K_{i+1} \to \bar{K}$ be a K-embedding. By the induction hypothesis, $\sigma(K_i) = K_i$. As K_{i+1} is an unramified ℓ-extension over K_i such that all places in T_i split, the same holds for $\sigma(K_{i+1})$. Therefore, $\sigma(K_{i+1}) \subseteq K_{i+1}$ since K_{i+1} is maximal with respect to these properties. This completes the induction. □

Our aim is to find conditions that guarantee G to be infinite. The strategy is as follows: suppose G is finite, then G is an ℓ-group, whose its generator rank $d_\ell(G)$ and relation rank $r_\ell(G)$ satisfy the Golod-Shafarevich inequality (Theorem 5.6). The generator rank of G is at least that of its first level $\mathrm{Gal}(K_1/K)$, which is the ℓ-rank of the T-class group. That is,

$$d_\ell(G) \geq d_\ell(Cl_T(K)).$$

In general it is difficult to estimate the ℓ-rank of the T-class group. One way to do this is to use Schoof's genus theory [72]. The following is an improved version of Schoof's result due to Niedierreiter and Xing [64].

Theorem 8.13. *Let $K/\mathbb{F}_q$ be a function field, which is a finite abelian extension of another function field $k/\mathbb{F}_q$ with Galois group H. Let T be a set of rational places in K and T_k be its underset in k. Then for any prime ℓ, we have*

$$d_\ell(Cl_T(K)) \geq \sum_{\mathfrak{p}\in\mathbb{P}_k} d_\ell(H_\mathfrak{p}) - (|T_k| - 1 + \epsilon_\ell(q)) - d_\ell(H),$$

where $H_\mathfrak{p}$ is the inertia group of the place $\mathfrak{p}$ in K/k, and

$$\epsilon_\ell(q) = \begin{cases} 1 & , \ \ell | q-1, \\ 0 & , \ \textit{otherwise.} \end{cases}$$

On the other hand, the difference between the relation rank and the generator rank cannot be too large. This is given by the classical Shafarevich inequality. See [47] for a proof.

Theorem 8.14. *If T is a non-empty set of rational places of a function field $K/\mathbb{F}_q$, and if G is the Galois group of the class field tower over K, then*

$$r_\ell(G) - d_\ell(G) \leq |T| - 1 + \epsilon_\ell(q).$$

Here $\epsilon_\ell(q)$ is defined as in Theorem 8.13.

Combining the inequalities in Theorem 8.13, Theorem 8.14 and Golod-Shafarevich, one may sometimes obtain a contradiction that G cannot satisfy all of them. This implies that G is infinite and hence our tower is infinite. For instance, in the case of K/k being cyclic of order ℓ in Theorem 8.13, Schoof [71] has worked out the details and obtained the following.

Proposition 8.15 (Schoof)**.** *Let $K/\mathbb{F}_q$ be a function field that is a cyclic extension of degree ℓ over a field k. Let T be a set of rational places in K with underset T_k in k, and let ρ be the number of places in k that*

are ramified in K. If

$$\rho \geq \begin{cases} 3 + |T_k| + 2\sqrt{|T|+1} & , \ \ell | q-1, \\ 3 + |T_k| + 2\sqrt{|T|} & , \ \textit{otherwise.} \end{cases}$$

then K has an infinite class field tower.

We end this chapter by giving an example of how we can construct infinite class field tower and obtain lower bounds for the Ihara constant.

Example 8.16 (Xing-Yeo [95])**.** Let $q = 2$. We outline how to obtain the lower bound

$$A(2) \geq 97/376 = 0.257979\ldots.$$

From the rational function field $F = \mathbb{F}_2(x)$ we construct two fields K and L, whose existence are guaranteed by the cyclotomic theory (see [69, Chap. 12] for details). The field K is a degree 24 abelian extension of F such that P_∞ and the place (x) splits completely, while the place $(x^4 + x^3 + x^2 + x + 1)$ is totally ramified. It has genus $g(K) = 65$. The field L is a degree 4 elementary abelian extension of F such that P_∞ splits completely and the place (x) is totally ramified. We then form the compositum KL.

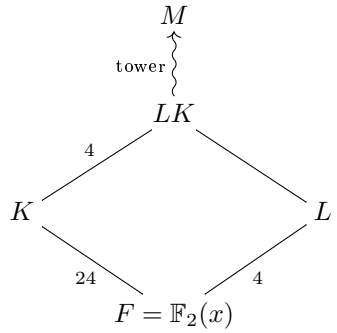


Figure 8.1: Field extensions in Xing-Yeo's construction

It can be calculated that $g(KL) = 377$. Denote by G the Galois group of the tower. As (x) is unramified in K/F, we have $K \cap L = F$. So $H = \mathrm{Gal}(KL/K) \cong (\mathbb{Z}/2\mathbb{Z})^2$. The only places that ramify in KL/K are those above (x), and they are totally ramified. There are 24 of them, all of which have inertia group $(\mathbb{Z}/2\mathbb{Z})^2$ since they are totally ramified and the order of H is a power of the characteristic.

Now let T_K be the set consisting of 24 places in K lying above P_∞ and one place lying above (x), and let T be the set of places in KL lying above T_K. Thus $|T_K| = 25$ and $|T| = 97$. By Theorem 8.13 (substitute

KL in place of K and K in place of k in the theorem),

$$\begin{aligned} d_2(G) \geq d_2(Cl_T(K)) &\geq \sum_{\mathfrak{p}\in\mathbb{P}_K} d_2(H_\mathfrak{p}) - (|T_K| - 1) - d_2(H) \\ &= 24 \times 2 - (25 - 1) - 2 \\ &= 22. \end{aligned}$$

By Theorem 8.14, we have

$$r_2(G) - d_2(G) \leq 97. \tag{8.2}$$

However, if G were finite, then by Golod-Shafarevich (Theorem 5.6),

$$r_2(G) - d_2(G) > \frac{d_2(G)^2}{4} - d_2(G) \geq \frac{22^2}{4} - 22 = 99.$$

This is a contradiction to (8.2). Thus G is infinite, and KL has an infinite class field tower with splitting set T. By Proposition 8.11, we get the lower bound

$$A(2) \geq \frac{|T|}{g(KL) - 1} = \frac{97}{377 - 1} = \frac{97}{376}.$$

Chapter 9

New lower bounds for $A(2)$ and $A(3)$

The aim of this chapter is to give a way to construct some infinite unramified class field towers which give lower bounds for the Ihara constant $A(q)$. Our construction yields the following.

Theorem 9.1. *Let k be a function field of genus g over $\mathbb{F}_q$ of characteristic p, where $q = p^e$. Let S be a finite set of places of k, and for each $\mathfrak{p} \in S$, let $f_\mathfrak{p}$ denotes its degree and let $\nu_\mathfrak{p}$ be a positive integer. Form the conductor $\mathfrak{m} = \sum_{\mathfrak{p}\in S} \nu_\mathfrak{p}\mathfrak{p}$. For a set T of $t > 0$ rational places disjoint from S with $t \leq \sum_{\mathfrak{p}\in S} ef_\mathfrak{p}(\nu_\mathfrak{p} - 1 - [(\nu_\mathfrak{p} - 1)/p])$, let $K = k_\mathfrak{m}^T$ be the ray class field with conductor $\mathfrak{m}$ so that all places in T split completely. If t satisfies the inequality*

$$(1 + \sum_{\mathfrak{p}\in S} ef_\mathfrak{p}(\nu_\mathfrak{p} - 1 - [(\nu_\mathfrak{p} - 1)/p]) - t)^2 \\ - 2\sum_{\mathfrak{p}\in S} ef_\mathfrak{p}(\nu_\mathfrak{p} - 1)(ef_\mathfrak{p}(\nu_\mathfrak{p} - 1) + 1) - 4\sum_{\mathfrak{p}\in S} ef_\mathfrak{p}(\nu_\mathfrak{p} - 1 - [(\nu_\mathfrak{p} - 1)/p]) \geq 0, \quad (9.1)$$

then the (T, p)-class field tower L/K is infinite, and we have

$$A(q) \geq \frac{t}{g - 1 + \frac{1}{2[K:k]} \sum_\chi \deg \mathfrak{f}_\chi},$$

where χ runs through the characters of $\mathrm{Gal}(K/k)$.

In general it may be difficult to determine exactly the degrees of the conductors for the characters of the group $\mathrm{Gal}(K/k)$, but we know that the conductors are bounded by $\mathfrak{m} = \sum_{\mathfrak{p}\in S} \nu_\mathfrak{p}\mathfrak{p}$ and their degrees by $\deg \mathfrak{m} = \sum_{\mathfrak{p}\in S} f_\mathfrak{p}\nu_\mathfrak{p}$. Therefore, we obtain the following corollary, which is slightly weaker than Theorem 9.1, but has the advantage of being easier to use.

Corollary 9.2. *Assumptions and settings as in Theorem 9.1. We have*

$$A(q) \geq \frac{t}{g - 1 + \frac{1}{2}\sum_{\mathfrak{p}\in S} f_\mathfrak{p}\nu_\mathfrak{p}}.$$

In particular, we improve the lower bounds for $A(2)$ and $A(3)$.

Theorem 9.3.

$$A(2) \geq 0.316999\ldots.$$

Theorem 9.4.

$$A(3) \geq 0.492876\ldots.$$

9.1 The idea of Kuhnt

Let K be a function field over $\mathbb{F}_q$ and fix a prime ℓ. Let G' be the Galois group of the ℓ-class field tower L above K. In the previous chapter we see that the class field tower method relies on some estimations of the generator rank and relation rank of G'. One of the estimations involves genus theory, which estimates the generator rank of the T-class group $Cl_T(K)$ by considering a subfield k of K. If K/k has enough ramification, then the ℓ-rank of $Cl_T(K)$ will be large. In practice, one chooses K/k to be an ℓ-extension since it is only the ℓ-rank of $\mathrm{Gal}(K/k)$ that matters in the estimate.

Kuhnt [49] observed that since both G' and $\mathrm{Gal}(K/k)$ are ℓ-groups, so is $G = \mathrm{Gal}(L/k)$. Hence, one may as well consider the group $\mathrm{Gal}(L/k)$ instead of $\mathrm{Gal}(L/K)$. This may give some improvement to the method. An example of his idea will be given in Example 9.6. In fact, the biggest advantage of considering G instead of G' (which Kuhnt may not be aware of) is that we can estimate the ℓ-rank of G by

$$d_\ell(G) \geq d_\ell(\mathrm{Gal}(K/k)), \tag{9.2}$$

but K/k is an extension that we are free to choose ourselves. Therefore, if we choose a base extension K/k with large ℓ-rank (that we have enough knowledge about it), this will allow us to circumvent the difficult estimation of the ℓ-rank of T-class group. When $\ell = p$ is the characteristic, the ray class fields are good supplies of such large p-extensions.

From now on, we fix $\ell = p$. The Golod-Shafarevich inequality certainly still works for $G = \mathrm{Gal}(L/k)$ as it is a p-group. If we use ray class fields as the base extension K/k, we may use (9.2) together with Proposition 6.13 for an estimate of $d_p(G)$ in place of the genus theory. We also need a replacement for the Shafarevich theorem (Theorem 8.14) for an estimate of $r_p(G) - d_p(G)$. This is done by Kuhnt [49].

Theorem 9.5 (Theorem 8.7 and 8.10 of Kuhnt [49])**.** *Let $L/K/k$ be a tower of Galois p-extensions of global function fields over a finite field. The extension K/k is finite, ramified at a set S of places of k and L/K is*

unramified. Let T_L be a nonempty, finite set of places in L and let $T_k = T_L \cap k$. Let $G = \mathrm{Gal}(L/k)$ and let

$$\Delta = r_p(G) - d_p(G) - \sum_{\mathfrak{p} \in S} (r_p(G_\mathfrak{p}) - d_p(G_\mathfrak{p})) - (|T_k| - 1) + d_p(\Delta_S),$$

where Δ_S is given by (6.3). If $\Delta > 0$, then there exists an unramified Galois p-extension $\tilde{L}/L$, in which T_L splits completely with $d_p(\mathrm{Gal}(\tilde{L}/L)) \geq \Delta$ and with the same constant field as L. In other words, if L is the maximal unramified p-extension of K (and T_L, T_k as above), then

$$r_p(G) - d_p(G) \leq \sum_{\mathfrak{p} \in S} (r_p(G_\mathfrak{p}) - d_p(G_\mathfrak{p})) + (|T_k| - 1) - d_p(\Delta_S).$$

The proof of this theorem is very long. Before we present the proof, we will first look at an example of how Kuhnt's idea can improve the lower bound for $A(2)$.

Example 9.6. We return to the setting of Example 8.16 and improve the lower bound for $A(2)$ there to

$$A(2) \geq 99/376 = 0.263298\ldots. \tag{9.3}$$

Refer to Figure 8.1, this time we let $G = \mathrm{Gal}(M/K)$. If T is the same as in the previous example, we have the same estimation of $d_2(G)$ by the genus theory except that we cannot subtract by $d_2(H)$ as it is now contained in our G. Thus $d_2(G) \geq 24$. By Corollary 5.4, if S is the set of ramified places in KL/K, we have for all $\mathfrak{p} \in S$,

$$r_2(G_\mathfrak{p}) - d_2(G_\mathfrak{p}) \leq r_2(I_\mathfrak{p}) = \frac{2(2+1)}{2} = 3,$$

where the penultimate step is by Lemma 5.5. However, if $\mathfrak{p} \in S \cap T_k$, we can do better. Since $\mathfrak{p}$ splits above KL in this case, we have $d_2(G) \leq 2$. So

$$r_2(G_\mathfrak{p}) - d_2(G_\mathfrak{p}) \leq \frac{2(2+1)}{2} - 2 = 1.$$

Note that $|S \cap T_k| = 1$, so by Theorem 9.5,

$$r_2(G) - d_2(G) \leq 3(23) + 1 + 24 = 94. \tag{9.4}$$

If G were finite, we have

$$r_2(G) - d_2(G) > \frac{d_2(G)^2}{4} - d \geq \frac{24^2}{4} - 24 = 120. \tag{9.5}$$

There is now a considerably larger gap between (9.4) and (9.5) (compared to the 97 and 99 in the previous example). This allows leeway to split more places. Let T_k' be the union of T_k with two more rational places above (x), and T' be the set of places above T_k'. We have $|T_k'| = 26$ and $|T'| = 98$. The inequalities become

$$\begin{aligned} d_2(G) &\geq 22, \\ r_2(G) - d_2(G) &\leq 92, \\ r_2(G) - d_2(G) &> 99. \end{aligned}$$

Therefore, the class field tower over KL is still infinite if we split the set T'. This gives the lower bound (9.3).

Proof of Theorem 9.5. First note that an argument similar to Proposition 8.12 shows that L/k is Galois. This justifies all the quotients and fixed field constructions in the proof.

(Step 1: Find proper solutions of local embedding problems.) Recall that $G = \mathrm{Gal}(L/k)$. Define the subgroup

$$H^2_{nr}(G, \mathbb{Z}/p\mathbb{Z}) = \{\epsilon \in H^2(G, \mathbb{Z}/p\mathbb{Z}) |\ res^G_{G_\mathfrak{p}}(\epsilon) \in H^2_{nr}(G_\mathfrak{p}, \mathbb{Z}/p\mathbb{Z})\ \forall \mathfrak{p} \in S\}.$$

By Proposition 7.9, for each nonzero $\epsilon \in H^2_{nr}(G, \mathbb{Z}/p\mathbb{Z})$ we can find a proper solution M_ϵ of the embedding problem $(L/K, \epsilon, S_L)$. Choose a basis $\epsilon_1, \ldots, \epsilon_n$ of $H^2_{nr}(G, \mathbb{Z}/p\mathbb{Z})$ and let N be the compositum of all the M_{ϵ_i}. Note that N is Galois over k since each M_{ϵ_i} is, and $\mathrm{Gal}(N/L)$ is central in $\mathrm{Gal}(N/k)$ because the G-action on $\mathbb{Z}/p\mathbb{Z}$ (which is the kernel of each embedding problem) is trivial. By Proposition 7.10, we have

$$d_p \,\mathrm{Gal}(N/L) = d_p H^2_{nr}(G, \mathbb{Z}/p\mathbb{Z}). \tag{9.6}$$

To calculate the p-rank of $H^2_{nr}(G, \mathbb{Z}/p\mathbb{Z})$, consider the restriction map

$$H^2(G, \mathbb{Z}/p\mathbb{Z}) \xrightarrow{\prod res} \prod_{\mathfrak{p} \in S} \left(H^2_{nr}(G_\mathfrak{p}, \mathbb{Z}/p\mathbb{Z}) \oplus H^2_{nr}(G_\mathfrak{p}, \mathbb{Z}/p\mathbb{Z})^{comp} \right),$$

where $H^2_{nr}(G_\mathfrak{p}, \mathbb{Z}/p\mathbb{Z})^{comp}$ is a complement (as a $\mathbb{F}_p$-vector space) of $H^2_{nr}(G_\mathfrak{p}, \mathbb{Z}/p\mathbb{Z})$ in $H^2(G_\mathfrak{p}, \mathbb{Z}/p\mathbb{Z})$. By Proposition 7.5, we have

$$d_p H^2_{nr}(G_\mathfrak{p}, \mathbb{Z}/p\mathbb{Z})^{comp} = \begin{cases} d_p H^2_{nr}(G_\mathfrak{p}, \mathbb{Z}/p\mathbb{Z}) - 1 & , \mathfrak{p} \in S_{nr}, \\ d_p H^2_{nr}(G_\mathfrak{p}, \mathbb{Z}/p\mathbb{Z}) & , \mathfrak{p} \notin S_{nr}. \end{cases}$$

Therefore, we have

$$\begin{aligned} & d_p H^2_{nr}(G, \mathbb{Z}/p\mathbb{Z}) \\ \geq\ & d_p H^2(G, \mathbb{Z}/p\mathbb{Z}) - \sum_{\mathfrak{p} \in S \setminus S_{nr}} d_p H^2(G_{\mathfrak{p}}, \mathbb{Z}/p\mathbb{Z}) - \sum_{\mathfrak{p} \in S_{nr}} \big(d_p H^2(G_{\mathfrak{p}}, \mathbb{Z}/p\mathbb{Z}) - 1\big) \\ =\ & r_p(G) - \sum_{\mathfrak{p} \in S \setminus S_{nr}} r_p(G_{\mathfrak{p}}) - \sum_{\mathfrak{p} \in S_{nr}} (r_p(G_{\mathfrak{p}}) - 1). \end{aligned}$$

Combining this with (9.6), we have

$$d_p \operatorname{Gal}(N/L) \geq r_p(G) - \sum_{\mathfrak{p} \in S \setminus S_{nr}} r_p(G_{\mathfrak{p}}) - \sum_{\mathfrak{p} \in S_{nr}} (r_p(G_{\mathfrak{p}}) - 1). \tag{9.7}$$

(Step 2: Remove the ramification exceeding the ramification depth of L/k.) Here, by "removing" the ramification of an extension N/L exceeding certain ramification depth ν, we mean to replace N by a subextension N_1 of N over L so that the ramification depth of N_1/L is bounded by ν.

For the extension L/k and $\mathfrak{p}$ a place in k, let $\nu_{\mathfrak{p}}$ be the ramification depth at $\mathfrak{p}$. Let S_L be the places in L lying above S, and ν_L be the lift of ν in S_L using (6.2). If the ramification of N obtained in Step 1 over L is still bounded by ν_L, go to step 3.

If not, let $\mathfrak{q}$ be a place in L so that N/L has ramification depth at $\mathfrak{q}$ exceeding $\nu_{L,\mathfrak{q}}$. For any place $\mathfrak{p}$ in S, let $L_{\mathfrak{p}}^{nr}$ be the maximal unramified subextension of $L_{\mathfrak{p}}/k_{\mathfrak{p}}$. Since the extension N/L obtained in Step 1 comes from $H^2_{nr}(G, \mathbb{Z}/p\mathbb{Z})$, the ramification index of any place $\mathfrak{p} \in S$ over L is at most p. Hence, we have $N_{\mathfrak{p}}/L_{\mathfrak{p}} = N'_{\mathfrak{p}}L_{\mathfrak{p}}/L_{\mathfrak{p}}$ for some $N'_{\mathfrak{p}}$ elementary abelian over $L_{\mathfrak{p}}^{nr}$. Let $n_{\mathfrak{p}}$ be the ramification depth of $N'_{\mathfrak{p}}/L_{\mathfrak{p}}^{nr}$. Then $n_{\mathfrak{p}} - 1$ is the highest ramification break of the extension. Since $L_{\mathfrak{p}}^{nr}/k_{\mathfrak{p}}$ is unramified, $n_{\mathfrak{p}} - 1$ is also the highest ramification break of $N'_{\mathfrak{p}}/k_{\mathfrak{p}}$.

Let M_1 be the compositum of N with all elementary abelian p-extensions of K ramified at the same places as N/L of depth at most $n_{\mathfrak{p}}$ for all $\mathfrak{p} \neq \mathfrak{q}$ and of exact depth $n_{\mathfrak{q}}$ at $\mathfrak{q}$. By Lemma 6.8, this does not change the ramification depth of any local extensions. In particular, we have $M_{1,\mathfrak{p}}/L_{\mathfrak{p}} = M'_{1,\mathfrak{p}}L_{\mathfrak{p}}/L_{\mathfrak{p}}$, with $M'_{1,\mathfrak{p}}/L_{\mathfrak{p}}^{nr}$ elementary abelian. The tower of the local fields are as shown in Figure 9.1.

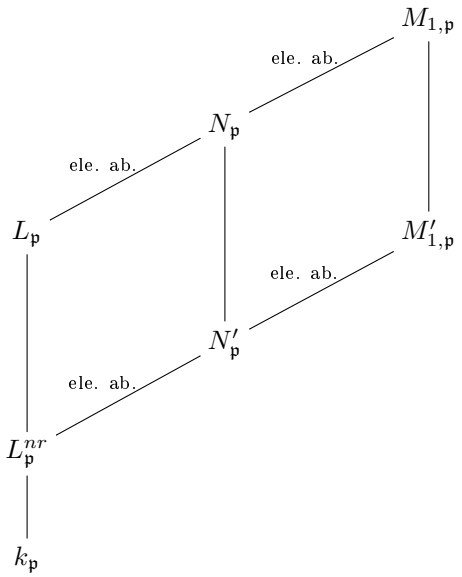


Figure 9.1: The tower of fields in Step 2.

Since $H = \mathrm{Gal}(M'_{1,\mathfrak{p}}/L^{nr}_{\mathfrak{p}})$ is abelian, the upper ramification group $H^{n_{\mathfrak{q}}-1}$ at $\mathfrak{q}$ has p-rank at most $e \cdot f_{\mathfrak{q}}$ by [74, Prop. IV.7] (here e is defined as in 6.18, and $f_{\mathfrak{q}}$ is the degree of $\mathfrak{q}$). There exists a subgroup H' of $G_1 = \mathrm{Gal}(M_1/k)$ which restricts isomorphically to $H^{n_{\mathfrak{q}}-1}$. Since G_1 is central in $\mathrm{Gal}(M_1/k)$, the subgroup H' is normal in $\mathrm{Gal}(M_1/k)$. By Theorem 6.18, the fixed field under H' is an extension M_2 of L with p-rank

$$\begin{aligned}
& d_p(\mathrm{Gal}(M_2/L) \\
= \; & d_p(\mathrm{Gal}(N/L)) + d_p G_{(S,\{n_{\mathfrak{p}}\}_{\mathfrak{p}})} - d_p G_{(S,\{\{n_{\mathfrak{p}}\}_{\mathfrak{p}\neq\mathfrak{q}},n_{\mathfrak{q}}-1\})} - d_p(H') \\
\geq \; & d_p(\mathrm{Gal}(N/L)) + 1 + \Delta_{(S,\{n_{\mathfrak{p}}\}_{\mathfrak{p}})} + e\sum_{\mathfrak{p}\in S} f_{\mathfrak{p}}(n_{\mathfrak{p}} - 1 - [(n_{\mathfrak{p}}-1)/p]) \\
& \quad - 1 - \Delta_{(S,\{\{n_{\mathfrak{p}}\}_{\mathfrak{p}\neq\mathfrak{q}},n_{\mathfrak{q}}-1\})} - e\sum_{\mathfrak{p}\neq\mathfrak{q}} f_{\mathfrak{p}}(n_{\mathfrak{p}} - 1 - [(n_{\mathfrak{p}}-1)/p]) \\
& \quad\quad - e\cdot f_{\mathfrak{q}}((n_{\mathfrak{q}}-1) + 1 + [(n_{\mathfrak{q}}-2)/p]) - e\cdot f_{\mathfrak{q}} \qquad (9.8) \\
= \; & d_p(\mathrm{Gal}(N/L)) + \Delta_{(S,\{n_{\mathfrak{p}}\}_{\mathfrak{p}})} - \Delta_{(S,\{\{n_{\mathfrak{p}}\}_{\mathfrak{p}\neq\mathfrak{q}},n_{\mathfrak{q}}-1\})} \\
& \quad + [(n_{\mathfrak{q}}-2)/p] - [(n_{\mathfrak{q}}-1)/p] \\
= \; & d_p(\mathrm{Gal}(N/L)) + \Delta_{(S,\{n_{\mathfrak{p}}\}_{\mathfrak{p}})} - \Delta_{(S,\{\{n_{\mathfrak{p}}\}_{\mathfrak{p}\neq\mathfrak{q}},n_{\mathfrak{q}}-1\})}.
\end{aligned}$$

The reason for the last step is as follows. As $N'_{\mathfrak{p}}/L_{\mathfrak{p}}$ is elementary abelian, Lemma 6.9 shows that $p \nmid (n_{\mathfrak{p}}-1)$. Hence $[(n_{\mathfrak{q}}-1)/p] = [(n_{\mathfrak{q}}-2)/p]$.

By our construction, M_2 has a lower ramification depth than N at $\mathfrak{q}$, and the ramification depths at

other $\mathfrak{p} \neq \mathfrak{q}$ in M_2 is at most that of N. Repeat the process from the beginning of step 2 with M_2 in place of N, until all ramification of N/L exceeding the depth ν has been removed. Call the resulting extension N_1.

Using the filtration

$$\Delta_S \subseteq \cdots \subseteq \Delta_{S,\{n_\mathfrak{p}\}_\mathfrak{p}} \subseteq \Delta_{(S,\{\{n_\mathfrak{p}\}_{\mathfrak{p}\neq\mathfrak{q}},n_\mathfrak{q}-1\})} \cdots \subseteq \Delta_{S_k,\nu},$$

we get

$$d_p(\mathrm{Gal}(N_1/L)) \geq d_p(\mathrm{Gal}(N/L)) - (d_p(\Delta_{S_k,\nu}) - d_p(\Delta_S)). \tag{9.9}$$

Finally, take the compositum M of N_1 with extensions of K ramified of depth bounded by ν and not already contained in L/k. The depth of the ramification in M is the same as that of N_1, and

$$d_p(\mathrm{Gal}(M/L)) \geq d_p(\mathrm{Gal}(N_1/L)) + d_p(G_{S,\nu}) - d_p(G). \tag{9.10}$$

Combining (9.8), (9.9), (9.10) above and (9.7) in step 1, we get

$$d_p(\mathrm{Gal}(M/L)) \geq r_p(G) - d_p(G) - \sum_{\mathfrak{p}\in S\setminus S_{nr}} r_p(G_\mathfrak{p}) - \sum_{\mathfrak{p}\in S_{nr}} (r_p(G_\mathfrak{p}) - 1) + d_p(G_{S,\nu}) + d_p\Delta_S - d_p\Delta_{S,\nu}. \tag{9.11}$$

Note that by our construction, the extension M/L is central over L/k.

(Step 3: Remove the remaining ramification above L.) Let $L_\mathfrak{p}^{ab}$ be the maximal abelian subextension of $L_\mathfrak{p}/k_\mathfrak{p}$, and let $G_\mathfrak{p}^{ab}$ be its Galois group. Let $I_\mathfrak{p}$ and $I_\mathfrak{p}^{ab}$ be the inertia group at $\mathfrak{p}$ of $L_\mathfrak{p}/k_\mathfrak{p}$ and $L_\mathfrak{p}^{ab}/k_\mathfrak{p}$ respectively. Let $I_\mathfrak{p}^{(p)} = I_\mathfrak{p}^{ab}/(I_\mathfrak{p}^{ab})^p$ be the maximal elementary abelian quotient of $I_\mathfrak{p}^{ab}$. Since M/L is central over L/k, we have $M_\mathfrak{p}/L_\mathfrak{p} = M'_\mathfrak{p}L_\mathfrak{p}/L_\mathfrak{p}$ with $M'_\mathfrak{p}/k_\mathfrak{p}$ abelian. Let $L_\mathfrak{p}^{nr}$ be the maximal unramified subextension of $L_\mathfrak{p}^{ab}/k_\mathfrak{p}$, and let $L_\mathfrak{p}^{(p)}$ be the extension of $L_\mathfrak{p}^{nr}$ corresponding to $I_\mathfrak{p}^{(p)}$. Then $M'_\mathfrak{p}L_\mathfrak{p}^{(p)}/L_\mathfrak{p}^{nr}$ is elementary abelian. Since this is Galois, we can take the fixed field of a complement of the inertia group of $M'_\mathfrak{p}L_\mathfrak{p}^{(p)}/L_\mathfrak{p}^{nr}$. Let $M_\mathfrak{p}^{'r}$ be the resulting extension. The tower of fields is shown in Figure 9.2.

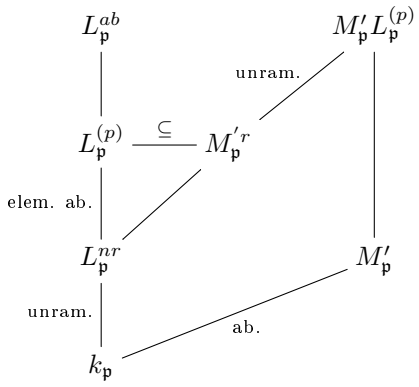


Figure 9.2: The tower of fields in Step 3.

The extension $M_{\mathfrak{p}}^{'r}/L_{\mathfrak{p}}^{nr}$ is totally ramified and elementary abelian. By Lemma 6.11, we have

$$d_p(\mathrm{Gal}(M_{\mathfrak{p}}^{'r}/L_{\mathfrak{p}}^{nr})) \leq e \cdot \deg \mathfrak{p} \cdot (\nu_{\mathfrak{p}} - 1 - [(\nu_{\mathfrak{p}} - 1)/p]). \tag{9.12}$$

Next, let N' be the field extension of L which remains after removing the ramification above K at all $\mathfrak{p}$ (by taking the fixed fields of the preimages of $\mathrm{Gal}(M_{\mathfrak{p}}^{'r}/L_{\mathfrak{p}}^{(p)})$ for all p). We can estimate the drop in global p-rank using the formula

$$d_p(\mathrm{Gal}(M_{\mathfrak{p}}^{'r}/L_{\mathfrak{p}}(p))) = d_p(\mathrm{Gal}(M_{\mathfrak{p}}^{'r}/L_{\mathfrak{p}}^{nr})) - d_p(I_{\mathfrak{p}}^{(p)}), \tag{9.13}$$

and

$$\begin{aligned} d_p(I_{\mathfrak{p}}^{(p)}) = d_p(I_{\mathfrak{p}}^{ab}/(I_{\mathfrak{p}}^{ab})^p) &= d_p(I_{\mathfrak{p}}^{ab}) \\ &= \begin{cases} d_p(G_{\mathfrak{p}}) - 1 & , \mathfrak{p} \in S_{nr}, \\ d_p(G_{\mathfrak{p}}) & , \mathfrak{p} \in S \backslash S_{nr}. \end{cases} \end{aligned} \tag{9.14}$$

The last formula is by Remark 7.4. We have

$$\begin{aligned}
& d_p(\mathrm{Gal}(N'/L)) \\
\geq\ & d_p(\mathrm{Gal}(M/L)) - \sum_{\mathfrak{p}\in S} d_p(\mathrm{Gal}(M_{\mathfrak{p}}^{'r}/L_{\mathfrak{p}}^{(p)})) \\
=\ & d_p(\mathrm{Gal}(M/L)) - \sum_{\mathfrak{p}\in S} d_p(\mathrm{Gal}(M_{\mathfrak{p}}^{'r}/L_{\mathfrak{p}}^{nr})) - d_p(I_{\mathfrak{p}}^{(p)}) \quad \text{(by (9.13))} \\
\geq\ & d_p(\mathrm{Gal}(M/L)) - e\cdot\sum_{\mathfrak{p}\in S}\deg\mathfrak{p}\cdot(\nu_{\mathfrak{p}} - 1 - [(\nu_{\mathfrak{p}}-1)/p]) \\
& \qquad + \sum_{\mathfrak{p}\in S} d_p(I_{\mathfrak{p}}^{(p)}) \quad \text{(by (9.12))} \\
=\ & d_p(\mathrm{Gal}(M/L)) - (d_p(G_{S,\nu}) - 1 - d_p(\Delta_{S,\nu})) + \sum_{\mathfrak{p}\in S} d_p(I_{\mathfrak{p}}^{(p)}) \\
\geq\ & r_p(G) - d_p(G) - \sum_{\mathfrak{p}\in S\setminus S_{nr}} r_p(G_{\mathfrak{p}}) - \sum_{\mathfrak{p}\in S_{nr}} (r_p(G_{\mathfrak{p}}) - 1) \\
& \qquad + d_p\Delta_S + 1 + \sum_{\mathfrak{p}\in S} d_p(I_{\mathfrak{p}}^{(p)}) \quad \text{(by (9.11))} \\
=\ & r_p(G) - d_p(G) - \sum_{\mathfrak{p}\in S\setminus S_{nr}} (r_p(G_{\mathfrak{p}}) - d_p(G_{\mathfrak{p}})) \\
& \qquad - \sum_{\mathfrak{p}\in S_{nr}} (r_p(G_{\mathfrak{p}}) - d_p(G_{\mathfrak{p}})) + d_p\Delta_S + 1 \quad \text{(by (9.14))} \\
=\ & r_p(G) - d_p(G) - \sum_{\mathfrak{p}\in S}(r_p(G_{\mathfrak{p}}) - d_p(G_{\mathfrak{p}})) + d_p\Delta_S + 1.
\end{aligned}$$

Finally, to ensure that the places in T_k split completely, we replace N' by the fixed field $\tilde{L}$ of the Frobenius of the places in T_k. We have $d_p(\mathrm{Gal}(\tilde{L}/L) \geq d_p(\mathrm{Gal}(N'/L)) - |T_k|$. The theorem follows. □

9.2 Construction of the tower

In this section, we describe our tower construction and prove Theorem 9.1. To begin with, let k be a function field over $\mathbb{F}_q$, called the *base field*. Let g and N be the genus and the number of rational places of k respectively. Let S be a set of places which we allow to ramify, and let T be a set of degree one places disjoint from S, of cardinalities $s = |S|$ and $t = |T|$. Clearly we have $t \leq N$. Let $\mathfrak{m} = \sum_{\mathfrak{p}\in S}\nu_{\mathfrak{p}}\mathfrak{p}$, where $\nu_{\mathfrak{p}} \in \mathbb{N}$ for each $\mathfrak{p}$. For any place $\mathfrak{p}$ of k, denote by $f_{\mathfrak{p}}$ its degree. Let K' be the ray class field of conductor $\mathfrak{m}$, and let $K = k_T^{\mathfrak{m}}$ be the maximal subfield of K' such that all places in T splits completely.

Let T_K be the set of places above T in K. Now we build the (T_K, p)-class field tower on top of K, and let L be the union of the tower. Let $G = \mathrm{Gal}(L/k)$. The extension of fields is shown in the following diagram.

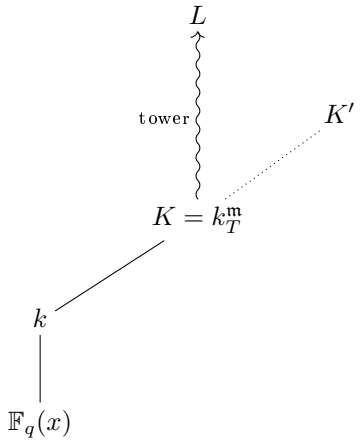


Figure 9.3: The tower construction

We determine the conditions to be met in order for the tower to be infinite. Suppose that G is finite, nontrivial and let $d = d_p(G)$, $r = r_p(G)$. From Proposition 6.13, we have

$$d \geq 1 + \sum_{\mathfrak{p} \in S} e f_{\mathfrak{p}} (\nu_{\mathfrak{p}} - 1 - [(\nu_{\mathfrak{p}} - 1)/p]) - t. \tag{9.15}$$

From Theorem 9.5 and Proposition 6.12, we have

$$r - d \leq \sum_{\mathfrak{p} \in S} \frac{(e f_{\mathfrak{p}} (\nu_{\mathfrak{p}} - 1))(e f_{\mathfrak{p}} (\nu_{\mathfrak{p}} - 1) + 1)}{2} + (t - 1). \tag{9.16}$$

Now G is infinite if (9.15) and (9.16) together yield a contradiction in the Golod-Shafarevich inequality

$$r - d > \frac{d^2}{4} - d.$$

This happens when

$$\frac{(1 + \sum_{\mathfrak{p} \in S} e f_{\mathfrak{p}} (\nu_{\mathfrak{p}} - 1 - [(\nu_{\mathfrak{p}} - 1)/p]) - t)^2}{4} - (1 + \sum_{\mathfrak{p} \in S} e f_{\mathfrak{p}} (\nu_{\mathfrak{p}} - 1 - [(\nu_{\mathfrak{p}} - 1)/p]) - t)$$
$$\geq \frac{(\sum_{\mathfrak{p} \in S} e f_{\mathfrak{p}} (\nu_{\mathfrak{p}} - 1))(e f_{\mathfrak{p}} (\nu_{\mathfrak{p}} - 1) + 1)}{2} + (t - 1),$$

which simplifies to

$$(1+\sum_{\mathfrak{p}\in S} ef_{\mathfrak{p}}(\nu_{\mathfrak{p}}-1-[(\nu_{\mathfrak{p}}-1)/p])-t)^2$$
$$-2\sum_{\mathfrak{p}\in S} ef_{\mathfrak{p}}(\nu_{\mathfrak{p}}-1)(ef_{\mathfrak{p}}(\nu_{\mathfrak{p}}-1)+1)-4\sum_{\mathfrak{p}\in S} ef_{\mathfrak{p}}(\nu_{\mathfrak{p}}-1-[(\nu_{\mathfrak{p}}-1)/p])\geq 0.$$

This is the condition (9.1) in Theorem 9.1.

Now suppose our tower is infinite (by a suitable choice of S, T and $\nu=(\nu_{\mathfrak{p}}:\mathfrak{p}\in S)$ so that (9.1) is satisfied), then we can calculate the lower bound of $A(q)$ given by this tower as follows. By Theorem 6.7, we have

$$2g(K)-2=[K:k](2g-2)+\sum_{\chi}\deg \mathfrak{f}_{\chi},$$

where χ runs through the characters of $\mathrm{Gal}(K/k)$. So,

$$g(K)-1=[K:k]\left(g-1+\frac{1}{2[K:k]}\sum_{\chi}\deg \mathfrak{f}_{\chi}\right). \tag{9.17}$$

In K, the number of places that splits in the tower L/K is $|T_K|=[K:k]t$. Therefore, by Proposition 8.11 and (9.17), we obtain the lower bound of $A(q)$ given by this tower.

$$A(q)\geq \frac{t[K:k]}{g(K)-1}=\frac{t}{g-1+\frac{1}{2[K:k]}\sum_{\chi}\deg \mathfrak{f}_{\chi}}.$$

This completes the proof of Theorem 9.1.

Remark 9.7. In Kuhnt's construction, Corollary 9.2 is obtained using a different argument, based on the "Ray class fields a la Hayes" (see [4, Example 1.5]), the tower in Figure 9.3 and the observation that

$$\frac{N(K')}{g(K')-1}\leq \frac{N(K)}{g(K)-1}\leq \frac{N(k)}{g(k)-1}.$$

Therefore, our theorem 9.1 can be viewed as an improvement to Kuhnt's result.

9.3 New lower bounds for $A(2)$ and $A(3)$

With Theorem 9.1 in hand, it remains for us to find a function field k so that the theorem is applicable. For this we look for function fields with many rational places with respect to their genus and with sufficiently many other places of small degree. For $q=2$, we construct two infinite towers. For the first tower we start

with the function field $E = \mathbb{F}_2(x, y)$ of the elliptic curve $y^2 + y = x^3 + x$. Denoting by a_d the number of places of degree d, we have

$$(a_d(E) : d \geq 1) = (5, 0, 0, 5, 4, 10, 20, 25, \ldots), \qquad g(E) = 1.$$

Let P_4 and P_5 be places of E of degree 4 and 5 respectively, and let E' be the ray class field of conductor $2P_4+2P_5$ in which all 5 rational places of E split completely. By Proposition 6.13, we have $d_2(\mathrm{Gal}(E'/E)) \geq 1 + 4 + 5 - 5 = 5$. Thus there is a subfield k of E' so that all the 5 rational places of E split completely and $\mathrm{Gal}(k/E)$ is an elementary abelian group of order 32. In particular $a_1(k) = 32 \cdot 5 = 160$. To calculate the genus of k, we use Theorem 6.7. One can show that there is no proper extension of E with conductor $2P_4$ so that all 5 rational places split. In k/E, there is a unique degree 2 subextension of conductor $2P_5$. The characters for the remaining degree 2 subextensions have conductor $2P_4 + 2P_5$. Hence $2g(k) - 2 = 32(0) + 1 \cdot 10 + 30 \cdot 18$, and $g(k) = 276$. To apply Theorem 9.1, we need a suitable set S of places to ramify. For this we analyse the places of small degree. There is a unique place of degree 5 in k above P_5, which is fully ramified in k/E. Notice that the extension k/E is elementary abelian and therefore it is a compositum of degree 2 Artin-Schreier extensions (see [80, Appendix A.13]). An explicit model for k is given by the compositum of the extensions $E(v)$ with

$$v^2 + ((x^2 + x)(xy + x + y) + 1)v = (x^2 + x)h,$$

where h is in the span of the functions $\{1, x, y, x^2, x^3\}$. The unique degree 2 subextension C/E with conductor $2P_5$ corresponds to $h = x$. For the extensions C/E and k/E we have

$$(a_d(C) : d \geq 1) = (10, 0, 0, 0, 3, \ldots), \quad g(C) = 6.$$
$$(a_d(k) : d \geq 1) = (160, 0, 0, 0, 1, 0, 0, 65, 0, 48, \ldots), \quad g(k) = 276.$$

The five places of degree 4 in E are inert in C/E. The place of degree 8 above P_4 ramifies completely in k/C and the places above the other places of degree 4 split completely in k/C (because k/E is elementary abelian), giving a total of 65 degree 8 places for k. The two nonramified places of degree 5 in C each decompose into 8 places of degree 10 in k. Now let S consist of one degree 5 place, 27 degree 8 places, and one degree 10 place, let $\nu_{\mathfrak{p}} = 2$ for all $\mathfrak{p} \in S$, and form the conductor $\mathfrak{m} = \sum_{\mathfrak{p} \in S} 2\mathfrak{p}$. Then one can check easily that the inequality (9.1) is satisfied for $t = |T| = 160$ and the class field tower of $K = k_T^{\mathfrak{m}}$ is infinite.

With Corollary 9.2 we find

$$A(2) \geq \frac{160}{276 - 1 + \frac{1}{2} \cdot 2 \cdot (1 \cdot 5 + 27 \cdot 8 + 1 \cdot 10)} = 80/253 = 0.316205\ldots.$$

The place of degree 5 contributes to a fraction of at most 31/32 of the characters for K/k, a place of degree 8 to a fraction of at most 255/256, and the place of degree 10 to a fraction of at most 1023/1024. Using this as an upper bound for the average conductor, Theorem 9.1 yields

$$\begin{aligned} A(2) &\geq \frac{160}{276 - 1 + \frac{1}{2} \cdot 2 \cdot (1 \cdot 5\,(1 - 2^{-5}) + 27 \cdot 8\,(1 - 2^{-8}) + 1 \cdot 10\,(1 - 2^{-10}))} \\ &= \frac{2^{14}}{2^9 \cdot 101 - 1} = 0.316837 > 32/101. \end{aligned}$$

We have shown

Proposition 9.8. *Let $E = \mathbb{F}_2(x, y)$ for $y^2 + y = x^3 + x$. For each $n \geq 0$, there exists a function field of degree 2^n over E with $N = 5 \cdot 2^n$ rational places and with genus g such that $N/g \geq 0.316837$.*

We construct a second tower to prove Theorem 9.3. Let H be the degree two extension of the rational function field with conductor $2P_3$, P_3 a place of degree 3, so that all 3 rational places split. A model for $H = \mathbb{F}_2(x, y)$ is given by $y^2 + (x^3 + x + 1)y = x^2 + x$. We have

$$(a_d(H) : d \geq 1) = (6, 0, 1, 1, 6, \ldots), \quad g(H) = 2.$$

For two places P_5 and P_5' of degree 5, let k/H be an abelian extension of type 2^5 with conductor $2P_5 + 2P_5'$ so that all 6 rational places split completely. Thus $a_1(k) = 32 \cdot 6 = 192$, and $2g(k) - 2 = 32(2) + 31 \cdot 20$ shows that $g(k) = 343$. An explicit model for k is given by the compositum of the extensions $E(v)$ with

$$v^2 + (x^5 + x^2 + 1)v = (x^2 + x)h,$$

where h is in the span of the functions $\{1, x, x^2, y, y^2\}$. We have

$$(a_d(k) : d \geq 1) = (192, 0, 0, 0, 2, 16, 0, 16, 0, 64, \ldots), \quad g(k) = 343.$$

Let the set S consist of 2 places of degree 5, 16 places of degree 6, 15 places of degree 8, and 4 places of

degree 10. For $\mathfrak{m} = \sum_{\mathfrak{p}\in S} 2\mathfrak{p}$, and for $|T| = 192$, the field $K = k_T^{\mathfrak{m}}$ has an infinite class field tower and

$$A(2) \geq \frac{192}{343 - 1 + \frac{1}{2}\cdot 2\cdot(2\cdot 5 + 16\cdot 6 + 15\cdot 8 + 4\cdot 10)} = 6/19 = 0.315789\ldots.$$

As before, using

$$\mathfrak{f}' = 2\cdot(2\cdot 5\,(1-2^{-5}) + 16\cdot 6\,(1-2^{-6}) + 15\cdot 8\,(1-2^{-8}) + 4\cdot 10\,(1-2^{-10}))$$

as an upper bound for the average conductor of K/k, Theorem 9.1 yields

$$A(2) \geq \frac{192}{343 - 1 + \frac{1}{2}\mathfrak{f}'} \geq 0.316999\ldots.$$

We have shown

Proposition 9.9. *For each $n \geq 0$, there exists a function field of degree 2^n over $\mathbb{F}_2(x)$ with $N = 3\cdot 2^n$ rational places and with genus g such that $N/g \geq 0.316999$.*

Now we turn our attention to $q = 3$. Again we consider the function field E of a maximal elliptic curve. This time we take $E = \mathbb{F}_3(x,y)$ with $y^2 = x^3 - x + 1$. We have $g(E) = 1$ and $(a_i(E) : i \geq 1) = (7, 0, 7, 21, 42, \ldots)$. Let P_5 be one of the degree 5 places of E and let E' to be the ray class field of E of conductor $3P_5$ so that all 7 rational places of E split completely. By Proposition 6.13, we have $d_3(\mathrm{Gal}(E'/E)) \geq 1 + 2\cdot 5 - 7 = 4$. Thus there is a subfield k of E' so that all the 7 rational places of E split completely and k/E is of type 3^4. In particular $[k : E] = 81$ and $a_1(k) = 81\cdot 7 = 567$. Using Theorem 6.7, we have $2g(k) - 2 = 3^4(0) + 80\cdot 3\cdot 5$, so that $g(k) = 601$. An explicit model of k is given by the compositum of the extensions $E(v)$ with

$$v^3 - (xy + x^2 - 1)^2 v = (x^3 - x)h,$$

where h is in the span of the functions $\{1, x, y, xy\}$. To see the splitting of the finite rational places we note that $(xy + x^2 - 1)^2 = (x^3 - x)(x^2 - y + x) + 1$. For the extension k we find

$$(a_d(k) : d \geq 1) = (567, 0, 0, 0, 1, 0, 0, 162, 1809), \quad g(k) = 601.$$

If we let S be a set of 46 places of degree 8 then, for $\mathfrak{m} = \sum_{\mathfrak{p}\in S} 3\mathfrak{p}$ and $|T| = 567$, the class field tower of $K = k_T^{\mathfrak{m}}$ is infinite with

$$A(3) \geq \frac{567}{601 - 1 + \frac{1}{2}\cdot 3\cdot(46\cdot 8)} = \frac{63}{128} = 0.4921875.$$

The same construction with S a set of one place of degree 5, 43 places of degree 8, and two places of degree 9, yields an infinite class field tower with $|T| = 567$. Using Theorem 9.1,

$$\begin{aligned} A(3) &\geq \frac{567}{601 - 1 + \frac{1}{2} \cdot 3 \cdot (1 \cdot 5\,(1 - 3^{-5}) + 43 \cdot 8\,(1 - 3^{-8}) + 2 \cdot 9\,(1 - 3^{-9}))} \\ &= 0.492876\ldots. \end{aligned}$$

Thus

Proposition 9.10. *Let $E = \mathbb{F}_3(x, y)$ for $y^2 = x^3 - x + 1$. For each $n \geq 0$, there exists a function field of degree 3^n over E with $N = 7 \cdot 3^n$ rational places and with genus g such that $N/g \geq 0.492876$.*

This proves Theorem 9.4.

9.4 Further remarks

9.4.1 Limitation of our construction

In our construction, we use ray class fields for the base extension K/k. This introduces wild ramifications, which bumps the genus $g(K)$ high. Therefore, although our construction works for any q, it can only produce good lower bounds for $A(q)$ when q is small. In particular, our method cannot produce lower bounds that are beyond certain limits.

Proposition 9.11. *Let $q = p^e$ be a prime power, and let*

$$L = \frac{t}{g - 1 + \frac{1}{2[K:k]} \sum_\chi \deg \mathfrak{f}_\chi}$$

be the lower bound for $A(q)$ we obtained in Theorem 9.1, then $L < 4e$.

Proof. The first condition in Theorem 9.1 is

$$\begin{aligned} t &\leq \sum_{\mathfrak{p} \in S} e f_{\mathfrak{p}} (\nu_{\mathfrak{p}} - 1 - [(\nu_{\mathfrak{p}} - 1)/p]) \\ &< e \sum_{\mathfrak{p} \in S} f_{\mathfrak{p}} \nu_{\mathfrak{p}}. \end{aligned}$$

On the other hand, we have for the average conductor

$$\sum_\chi \deg \mathfrak{f}_\chi \geq \frac{[K:k]}{2} \mathrm{cond}(K/k) = \frac{[K:k]}{2} \sum_{\mathfrak{p} \in S} f_{\mathfrak{p}} \nu_{\mathfrak{p}},$$

since there are at least half of the characters having a conductor exactly equals to $\mathrm{cond}(K/k)$. Therefore,

$$L = \frac{t}{g - 1 + \frac{1}{2[K:k]} \sum_{\chi} \deg \mathfrak{f}_{\chi}} < \frac{e \sum_{\mathfrak{p} \in S} f_{\mathfrak{p}} \nu_{\mathfrak{p}}}{\frac{1}{4} \sum_{\mathfrak{p} \in S} f_{\mathfrak{p}} \nu_{\mathfrak{p}}} = 4e.$$

□

In practice, our method improves the bound for $A(2)$ and $A(3)$, but falls short when $q = 5$. In such case, the best lower bound we find using out method is $A(5) \geq 0.691222\ldots$, which is less than the current best lower bound $A(5) \geq 0.727272\ldots$, obtained using the tame tower method [3].

9.4.2 Possible improvements

In this subsection, we discuss some possible ways to improve the bounds on $A(q)$.

The first one is a possible tame analogue of our construction. Let p be a prime. There are many variants of the class field tower method tailored for specific cases of $A(p)$. We observe that if p is very small, namely if $p = 2, 3$, the best lower bounds for $A(p)$ are obtained using unramified tower with a wildly ramified base. If p is of "medium size", say if $5 \leq p \leq 50$, the tame tower over a tame base is the current best approach. For p large, say $p > 50$, Serre's unramified towers over hyperelliptic curves remain the best.

This suggests that we may be able to improve the lower bound of $A(p)$ for larger p if we obtain a tame analogue of Kuhnt's method. Let ℓ be a prime that is different from the characteristic p. Kuhnt [49] already provides an estimate for $r_{\ell}(G) - d_{\ell}(G)$ in this situation (here, as usual, we set $G = \mathrm{Gal}(L/k)$. However, one needs to find a suitable tame base field k so that k has many rational places, $d_{\ell}(G)$ is large but the genus of the ground field $g(K)$ is still comparably small. To this end, our experiments reveal that the standard ray class field construction applied to this case will yield an equivalent theory to Theorem 8.13, which means no improvements in the theory level is possible if we simply employ the ray class fields as our base extensions. Note that a tame analogue of the construction also enable the possibility of having a tame tower instead of an unramified tower, which cannot be done in the wild ramification case.

Question 9.12. How do we construct tame ℓ-extensions with many rational places and large ℓ-rank, that beat those constructed by ray class fields?

Another possible improvement comes from understanding Kuhnt's Theorem 9.5. We are not able to use the full strength of the theorem since we do not have enough understanding of the term $d_p(\Delta_S)$, which concerns the p-th power of the ideal group. So a more detailed understanding of Δ_S will allow us to use the full strength of Theorem 9.5, and a possibility of improvement.

There are two possible improvements for Proposition 6.13. We estimate the p-rank of the ray class group of $k_T^{\mathfrak{m}}$ over k only by the idelic parts coming from the places that ramifies, but the ray class group also consists of a part coming from the T-class group $CL_T(k)$. If we have an estimate for the p-rank of $Cl_T(k)$, we can add that to the rank of the ray class group. On the other hand, experiments show that for a large ray class field extension with splitting set T, the Frobenius of the places in T need not be linearly independent. Therefore, knowing the linear dependence situation in the ray class group will also improve the estimate.

Finally, we remark that most efforts are devoted to improve the lower bounds for $A(q)$ when q is not a square. However, it might be the case that the upper bound is not sharp for such q. Let $q = p^r$ with $r \geq 3$ odd, some people think that $A(q)$ should be dominated by a constant multiple of $p^{(r-1)/2}$ [56]. If so, then the result of Garcia-Stichtenoth-Bassa-Beelen [25] may be close to the upper bound.

Chapter 10

Elliptic curves over function fields and their Selmer groups

In the last two chapters, we change context again and "move one dimension higher" to study elliptic curves over function fields. In particular, we study the Selmer group, which is closely related to the Mordell-Weil group of an elliptic curve and the Birch and Swinnerton-Dyer conjecture. Our primary reference is [77, 78], in which most of the theory over number fields such as $\mathbb{Q}$ can be translated word-by-word to the function field case. When separate treatments are required for the function field case, we will follow [87].

10.1 Elliptic curves over function fields

Let $q = p^e$ be a prime power, and K be a function field over $k = \mathbb{F}_q$. An *elliptic curve* E over K is a smooth, projective, absolutely irreducible curve of genus 1 over K having a distinguished rational point O, called the *base point*, which acts as the identity of the group law. Every elliptic curve can be written as a plane cubic curve defined by the Weierstrass equation

$$E: \ Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

with $a_1, \ldots, a_6 \in K$. The base point O is the unique point at infinity $[0:1:0]$. To simplify notations, we let $x = X/Z$ and $y = Y/Z$, and write E in affine form:

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6. \tag{10.1}$$

If the characteristic $p \neq 2, 3$, then we can put the equation in the form

$$y^2 = x^3 + Ax + B. \tag{10.2}$$

The *discriminant* Δ for (10.2) and the j-invariant j are by definition

$$\Delta = -16(4A^3 + 27B^2),$$
$$j = -1728\frac{(4A)^3}{\Delta},$$

and the *invariant differential* is

$$\omega = \frac{dx}{2y}.$$

We remark that there are similar formulas for $p = 2, 3$, but they are more complicated and we refer the reader to [78]. The following proposition characterizes when a cubic curve over $\mathbb{P}^2$ is an elliptic curve, and determines its $\bar{K}$ (the algebraic closure of K) isomorphism class. See [78] for a proof.

Proposition 10.1. *Let $E \subseteq \mathbb{P}^2$ be a cubic curve with discriminant Δ.*

1. *E is an elliptic curve (i.e. smooth over K) if and only if $\Delta \neq 0$.*
2. *Two elliptic curves E_1 and E_2 over K are isomorphic over $\bar{K}$ if and only if $j(E_1) = j(E_2)$.*

Denote by $E(K)$ the set of K-rational points on E. There is a group law on $E(K)$ making it an abelian group with identity O. The group law can be described as follows: write E as a cubic curve in $\mathbb{P}^2$, any line will cut E at 3 points P_1, P_2, P_3 (which need not be distinct). The group law is characterized by $P_1 + P_2 + P_3 = 0$.

The following definitions are specific to the elliptic curves over function fields.

Definition 10.2. Let E be an elliptic curve over $K/\mathbb{F}_q$.

1. E is said to be *constant* if there is an elliptic curve E_0 over $\mathbb{F}_q$ such that $E \cong E_0 \times_{\mathbb{F}_q} K$. That is, E can be defined over $\mathbb{F}_q$.
2. E is said to be *isotrivial* if there is a finite extension L of K such that E becomes constant over L.
3. E is *non-isotrivial* if it is not isotrivial.

The following proposition provides an easy way to check if E is isotrivial. Its proof is easy.

Proposition 10.3. *Let E be an elliptic curve over $K/\mathbb{F}_q$, then E is isotrivial if and only if $j(E) \in \bar{\mathbb{F}}_q$.*

Example 10.4. Let $K = \mathbb{F}_p(t)$ with $p > 3$. Define

$$E_1 : \ y^2 = x^3 + t^6$$
$$E_2 : \ y^2 = x^3 + t$$
$$E_3 : \ y^2 = x^3 + x + t.$$

Then E_1 is constant (it is isomorphic to the curve $E_1' : \ y^2 = x^3 + 1$), E_2 is isotrivial but nonconstant, while E_3 is non-isotrivial.

Let E_1 and E_2 be two elliptic curves over K. A *K-isogeny* from E_1 to E_2 is a surjective morphism of curves $\phi : E_1 \to E_2$ over K such that $\phi(O_{E_1}) = O_{E_2}$. It can be shown that a K-isogeny is automatically a group homomorphism between $E_1(K)$ and $E_2(K)$ [78, Theorem III.4.8]. If there is an isogeny between E_1 and E_2, we say that they are *isogenous*, and denote by $E_1 \sim E_2$. It can be shown that $\sim$ is an equivalence relation. The *degree* of an isogeny ϕ is the degree of ϕ as a morphism of curves (when ϕ is the zero map we make the convention by saying $\deg \phi = 0$). An isogeny of degree one is an *isomorphism*.

Example 10.5. One important example of an isogeny is the *multiplication-by-m* map. Let E be an elliptic curve and m be an integer. When $m > 0$, define

$$[m] : E \to E$$

by sending P to $[m](P) = P + P + \ldots + P$ (m times). When $m < 0$, we define $[m](P) = [-m](-P)$, and for $m = 0$, $[0](P)$ is the zero map sending every point on E to the base point O. The degree of $[m]$ is m^2, and its kernel, denoted by $E[m]$, is called the *m-torsion subgroup* of E.

Let $\phi : E_1 \to E_2$ be an isogeny of degree d. There is an unique isogeny $\hat{\phi} : E_2 \to E_1$ going the other way such that $\hat{\phi} \circ \phi = [d]$ on E_1 and $\phi \circ \hat{\phi} = [d]$ on E_2. The map $\hat{\phi}$ is called the *dual isogeny* of ϕ.

Example 10.6. Let $p = \mathrm{char}(K) \neq 2$, and let $a, b \in K$ with $b \neq 0$ and $r = a^2 - 4b \neq 0$. Consider the two elliptic curves

$$E_1 : \ y^2 = x^3 + ax^2 + bx,$$
$$E_2 : \ Y^2 = X^3 - 2aX^2 + rX.$$

There are isogenies of degree two connecting these two curves,

$$\phi : E_1 \to E_2, \qquad \hat{\phi} : E_2 \to E_1$$
$$(x, y) \mapsto \left(\frac{y^2}{x^2}, \frac{y(b - x^2)}{x^2} \right), \qquad (X, Y) \mapsto \left(\frac{Y^2}{4X^2}, \frac{Y(r - X^2)}{8X^2} \right).$$

It can be shown that the two isogenies ϕ and $\hat{\phi}$ are dual to each other.

Example 10.7. Let $p = 2$. Let E be an elliptic curve over K with equation

$$E: \ y^2 + a_1 xy = x^3 + a_2 x^2 + a_6,$$

where $a_1, a_6 \neq 0$. We have the Frobenius isogeny $\pi : E \to E^{(2)}$, where

$$E^{(2)}: \ y^2 + a_1^2 xy = x^3 + a_2^2 x^2 + a_6^2,$$

and $\pi(x, y) = (x^2, y^2)$. The degree of π is 2.

More generally, if $K/\mathbb{F}_q$ is a function field of characteristic p, and E is an elliptic curve over K with Weierstrass equation (10.1), define another elliptic curve $E^{(p)}$ by replacing in (10.1) the coefficients a_i by a_i^p. The Frobenius isogeny $\pi_p : E \to E^{(p)}$ with $\pi_p(x, y) = (x^p, y^p)$ is a degree p isogeny.

Note that $j(E^{(p)}) = j(E)^p$. So if E is not isotrivial, $E^{(p)}$ and E are not isomorphic. In this case, we can iterate π_p to obtain an infinite family of non-isomorphic elliptic curves that are all isogenous to E.

We remark that there is another very useful way to view an elliptic curve E over K. Let C be a smooth curve over $k = \mathbb{F}_q$ corresponding to K, then we have a map $E \twoheadrightarrow C$ which is a fibration of E over C. Thus we can also view E as an *elliptic surface* over k with the above fibration. We will not need this point of view in the thesis.

10.2 Rational points on elliptic curves over function fields

Given an elliptic curve E over K, one central question in the arithmetic of elliptic curves is to determine its group of K-rational points $E(K)$. An important result in this direction is the following theorem. See [52] for a proof.

Theorem 10.8 (Mordell-Weil-Lang-Néron)**.** *$E(K)$ is a finitely generated abelian group.*

By this theorem, we can write

$$E(K) \cong E_{\text{tors}}(K) \oplus \mathbb{Z}^r,$$

where $E_{\text{tors}}(K)$ is the torsion subgroup of E_K, and r is the *rank* of E. Note that $E_{\text{tors}}(K)$ is finite.

The torsion group is isomorphic to a group of the form $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, with $m \mid n$ and $p \nmid m$ (see [78]). Indeed, one can give uniform bounds for the orders of the torsion groups of all E/K that depend only on invariants of the field K. If E is constant, then $E \cong E_0 \times_k K$ for some elliptic curve E_0 over $k = \mathbb{F}_q$. Indeed,

$E_{\text{tors}}(K) \cong E_0(k)$, which has order bounded by $q + 1 + 2\sqrt{q}$. The case for E isotrivial is similar. For the non-isotrivial case, we have the following.

Proposition 10.9. *Let K be a function field over $\mathbb{F}_q$. There is a finite and effectively computable list of groups, depending only on $g(K)$ and q, such that any non-isotrivial elliptic curve E over K has its torsion group on the list.*

Proof. See [55]. □

On the other hand, the non-torsion part of E is more mysterious. Nevertheless, we know the following theorem about the rank. Note that the corresponding statement in the number field case is still a wide-open conjecture.

Theorem 10.10 (Tate-Shafarevich [83])**.** *Let K be a function field. There exist elliptic curves over K with arbitrarily large rank.*

We can define an L-function $L(E, s)$ attached to E similar to the number field case (see [77, 78]). One very deep conjecture that relates the rank of an elliptic curve E and its L-function is the Birch and Swinnerton-Dyer conjecture (or the BSD conjecture, in short).

Conjecture 10.11 (Birch and Swinnerton-Dyer)**.**

$$\text{rank } E(K) = \text{ord}_{s=1} L(E, s).$$

We remark that there is a more refined version of the BSD conjecture involving the Tate-Shafarevich group. Unlike the number field case, we know much more towards the conjecture. For instance, we have Rank $E(K) \leq \text{ord}_{s=1} L(E, s)$, and the BSD conjecture is true for isotrivial elliptic curves. See [87] for an account of recent developments towards the conjecture.

10.3 Selmer groups

Let E and E' be two elliptic curves over K, a function field of characteristic p. Let $\phi : E \to E'$ be an isogeny of degree prime to p, and denote by $E[\phi]$ its kernel. Fix a separable closure $\bar{K}$ of K, and let $G = \text{Gal}(\bar{K}/K)$, then we have an exact sequence of G-modules

$$0 \longrightarrow E[\phi] \longrightarrow E(\bar{K}) \xrightarrow{\phi} E'(\bar{K}) \longrightarrow 0.$$

Taking Galois cohomology and using some homological algebra, one obtains the following fundamental short exact sequence:

$$0 \longrightarrow E'(K)/\phi(E(K)) \longrightarrow H^1(G, E[\phi]) \longrightarrow H^1(G, E)[\phi] \longrightarrow 0.$$

We wish to understand the group $E'(K)/\phi(E(K))$, where in the case $\phi = [m]$ it becomes the weak Mordell-Weil group $E(K)/mE(K)$. This group is directly related to the problems of determining the rank of E and finding explicit generators of $E(K)$. To this end, we break down the cohomology groups by local considerations. For each (inequivalent) valuation v of K, fix an embedding $\bar{K} \subseteq \bar{K}_v$, and its decomposition group $G_v \subset G$. Then we have natural embeddings $E(\bar{K}) \hookrightarrow E(\bar{K}_v)$ and similarly for E'. The group G_v acts on the above completion, and yields (via the same machanism above) the following commutative diagram.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & E'(K)/\phi(E(K)) & \longrightarrow & H^1(G, E[\phi]) & \longrightarrow & H^1(G, E)[\phi] & \longrightarrow & 0 \\ & & \downarrow{\scriptstyle 0} & & \downarrow{\scriptstyle \pi_1} & & \downarrow{\scriptstyle \pi_2} & & \\ 0 & \longrightarrow & 0 & \longrightarrow & \prod_{v \in \mathbb{P}_K} H^1(G_v, E) & \longrightarrow & \prod_{v \in \mathbb{P}_K} H^1(G_v, E) & \longrightarrow & 0. \end{array}$$

Here the product runs through a set of valuations of K. The kernel of π_1 is called the *ϕ-Selmer group*, denoted by $Sel^{(\phi)}(E/K)$, and the kernel of π_2 is called the *Tate-Shafarevich group*, denoted by $Ш(E/K)$. When the degree of ϕ is a multiple of p, the Selmer group and the Tate-Shafarevich group can be defined similarly, using flat cohomology of K instead of Galois cohomology [88].

By the snake lemma, we get the short exact sequence

$$0 \longrightarrow E'(K)/\phi(E(K)) \longrightarrow Sel^{(\phi)}(E/K) \longrightarrow Ш(E/K)[\phi] \longrightarrow 0. \tag{10.3}$$

The Tate-Shafarevich group is a mysterious object. We still do not know whether it is finite or not, albeit the BSD conjecture predicts that it is finite with a square order. On the contrary, the Selmer group is a product of local objects, and is easier to handle.

Theorem 10.12. *The Selmer group $Sel^{(\phi)}(E/K)$ is finite.*

Proof. When $\deg \phi$ is not divisible by the characteristic p of K, the same proof as in [78, Chap. X] applies. The main idea is to use the finiteness of the class number and the Dirichlet unit theorem. The situation for $p \mid \deg \phi$ is more difficult and requires a different strategy. See [48] for the case $p = 2$ and [88, 91] for general p. □

In practice, the Selmer group can be effectively calculated in some cases using the method of *descent*.

Let $K = \mathbb{F}_q(t)$, fix some $a, b \in K$ and let $n \in K$ be a parameter. In the next chapter, we will compute the distribution of Selmer groups of the family of elliptic curves

$$E_n : \ y^2 = x(x + an)(x + bn)$$

over K for odd q, for a degree 2 isogeny ϕ.

Remark 10.13. The curve E_n occurs naturally as the quadratic twists of the general elliptic curve with full 2-torsion group,

$$E : \ y^2 = x(x + a)(x + b),$$

by a squarefree polynomial n.

Chapter 11

Distribution of Selmer groups of E_η

In this chapter, we will use the complete 2-descent method to compute the distribution of the ϕ-Selmer groups of the family of elliptic curves

$$E_n : \qquad y^2 = x(x+an)(x+bn) \tag{11.1}$$

over $K = \mathbb{F}_q(t)$ for odd q, with $a, b \in K$ fixed, $n \in K$ a parameter and $\phi : E_n \to E'_n$ as in Example 10.6. i.e.

$$E'_n : \qquad Y^2 = X^3 - 2(a+b)nX^2 + (a-b)^2n^2X,$$

and

$$\phi(x,y) = \left(\frac{y^2}{x^2}, \frac{y(abn^2 - x^2)}{x^2}\right).$$

Let $R = \mathbb{F}_q[t]$. Fix a positive integer N and coprime monic polynomials h, C. Define the set

$$S(N,h,C) = \{n \in R : \deg n = N, n \equiv h \pmod{C},\ n \text{ monic, square-free}\}. \tag{11.2}$$

In this chapter, we will investigate the asymptotic behaviour of the size of the Selmer group $Sel^{(\phi)}(E_n/K)$ for $n \in S(N,h,C)$ as N goes to infinity.

Theorem 11.1. *Let $a, b \in R$ with $ab(a-b) \neq 0$, $\deg(ab) \geq 1$ and ab not a square. Let*

$$C_0 = \prod_{\substack{P \in \mathbb{P}_K \\ P \mid ab(a-b)}} P,$$

and let $h, C \in R$ be coprime polynomials and $C_0 \mid C$. For a positive integer N and $n \in S(N,h,C)$, define $s(n,\phi)$ by

$$\left|Sel^{(\phi)}(E_n/K)\right| = 2^{s(n,\phi)},$$

where E_n is the elliptic curve (11.1). *Then*

$$s(n,\phi) \leq \omega(a-b)+1$$

for almost all $n \in S(N,h,C)$ as $N \to \infty$ (here $\omega(a-b)$ is the number of distinct prime divisors of the polynomial $a-b$).

11.1 Complete 2-descent

The complete 2-descent in number fields is explained in [78, Chapter X]. The same theory, with some slight modifications, can also be employed in the function field case when $\mathrm{char}(K) \neq 2$ (see also the lecture notes of Ulmer [87]). In our case of E_n, this can be done as follows.

For a square-free polynomial $n \in R$, define a finite set $S \subseteq \mathbf{P}_K$ by

$$S = \{P : P \mid ab(a-b)n\} \cup \{P_\infty\},$$

where P_∞ denotes the place at infinity corresponding to the pole of t. Let M be the multiplicative subgroup of K^*/K^{*2} generated by a quadratic nonresidue α modulo q and the primes dividing $(a-b)n$. For each $d \in M$, we have the homogeneous space C_d given by

$$C_d : \qquad dw^2 = t^4 - 2(a+b)\frac{n}{d}t^2z^2 + (a-b)^2\frac{n^2}{d^2}z^4.$$

The Selmer group $Sel^{(\phi)}(E_n/K)$ measures the possibility of C_d having non-trivial solutions in the local fields K_v for all $v \in S$. i.e.

$$Sel^{(\phi)}(E_n/K) \cong \{d \in M : C_d(K_v) \neq \mathbf{0}\ \forall v \in S\}.$$

Remark 11.2. If $v \notin S$, the homogeneous space C_d always has a non-trivial solution. In fact, for $v \notin S$, the reduction of C_d at v is a non-singular curve over a finite field, and therefore must contain a rational point by Weil's theorem (Theorem 3.1) since C_d has genus 1.

Remark 11.3. By (10.3), the Tate-Shafarevich group $Ш(E/K)$ corresponds to elements in M that have a non-trivial local solution for the homogeneous space C_d at all v, but fail to have a non-trivial global solution for C_d over K. In other words, the group $Ш(E/K)$ measures the failure of the Hasse principle for the elliptic curve E.

11.2 Lemmas on character sums

To analyze the sizes of the Selmer groups, we will follow the idea of Heath-Brown [41, 42] to express the sizes of the Selmer groups in terms of certain character sums. For this we will need the function field analogue of Heath-Brown's estimation.

For the rest of this chapter, we always assume that a sum over polynomials only runs through the monic polynomials that meet the summing criterions unless otherwise stated.

Recall that $\mu(n)$ is the Mobius function, and $\omega(n)$ is the number of distinct prime divisors of n.

Lemma 11.4 (Function field analogue of Lemma 4.2 in [98]). *Let c be a fixed rational number, and let N be a large positive integer. For any two relatively prime polynomials h, C and any non-principal character $\chi \pmod C$, we have*

$$\sum_{\substack{\deg n = N \\ GCD(n,C)=1}} \mu^2(n) c^{\omega(n)} \chi(n) = O(q^{N(\frac{1}{2}+\varepsilon)})$$

for any $\varepsilon > 0$.

Proof. We may assume that $c \neq 0$. Write $|c| = t/d$ with $t, d \in \mathbb{Z}$ and $GCD(t,d) = 1$. Let $S(N)$ be the sum in this lemma. For s with $\mathrm{Re}(s) > 1$, define

$$f(s) = \sum_{N=1}^{\infty} \frac{S(N)}{|n|^s},$$

where $|n| = q^{\deg n}$, then we have the Euler product expansion

$$f(s) = \prod_{P \nmid C} \left(1 + \frac{c\chi(P)}{|P|^s}\right).$$

Here the product over P runs through all monic irreducible polynomials in R that does not divide C. So,

$$\begin{aligned} f(s)^d &= \prod_{P|C} \left(1 + \frac{c\chi(P)}{|P|^s}\right)^{-d} \prod_{P} \left(1 + \frac{dc\chi(P)}{|P|^s} + \frac{d(d-1)c^2\chi^2(P)}{2\,|P|^{2s}} + \dots\right) \\ &= \prod_{P|C} \left(1 + \frac{c\chi(P)}{|P|^s}\right)^{-d} L(s,\chi)^{dc} g(s,c,\chi). \end{aligned} \tag{11.3}$$

Here $g(s,c,\chi)$ is holomorphic, non-vanishing and converges absolutely on the half-plane $\mathrm{Re}(s) > 1/2$. By Theorem 3.1, $L(s,\chi)$ is entire and non-vanishing for $\mathrm{Re}(s) > 1/2$. Thus in the region $\mathrm{Re}(s) > 1/2$, we have

a proper analytic branch of $L(s,\chi)^c g(s,c,\chi)^{\frac{1}{d}}$. Therefore, by (11.3), in the region $\mathrm{Re}(s) > 1/2$,

$$f(s) = \prod_{P|C} \left(1 + \frac{c\chi(P)}{|P|^s}\right)^{-1} L(s,\chi)^c g(s,c,\chi)^{\frac{1}{d}}.$$

Therefore, $f(s)$ is holomorphic for $\mathrm{Re}(s) > 1/2$. The desired estimation now follows from the Wiener-Ikehara Tauberian theorem (Theorem 2.21). □

We next deal with the sum $\sum_{\deg n=N} \gamma^{\omega(n)}$, where $\gamma > 0$. The Tauberian theorem is not applicable in this case, so we will turn to Lemma 2.22.

Lemma 11.5. *For any $\gamma > 0$ and $N \geq 1$, we have*

$$\sum_{\deg n=N} \gamma^{\omega(n)} \ll q^N N^{\gamma-1}.$$

Proof. Let $f(n) = \gamma^{\omega(n)}$. We need to show that both conditions in Lemma 2.22 are satisfied. For condition 1, we have

$$\sum_{\deg P=N} f(P) = \gamma \sum_{\deg P=n} 1 \leq 2\gamma \frac{q^N}{N}$$

by the prime number theorem over K. For condition 2, consider

$$\begin{aligned}
\sum_{P\in\mathbb{P}_K} \sum_{v\geq 2} \frac{f(P^v)}{|P|^v} \deg(P^v) &= \gamma \sum_P \deg P \sum_{v\geq 2} \frac{v}{q^v \deg P} \\
&\leq 2\gamma \sum_{j=1}^{\infty} q^j \sum_{v\geq 2} \frac{v}{q^{vj}} \\
&= 2\gamma \sum_{j=1}^{\infty} q^j \left(\frac{q^j - 2}{q^j(q^j-1)^2}\right) \\
&\leq 8\gamma \sum_{j=1}^{\infty} \frac{1}{q^j} \\
&= \frac{8\gamma}{q-1}.
\end{aligned}$$

Therefore, by Lemma 2.22, we have

$$\sum_{\deg n=N} \gamma^{\omega(n)} \ll \frac{q^N}{N} \sum_{\deg n\leq N} \frac{\gamma^{\omega(n)}}{|n|}. \tag{11.4}$$

The sum on the right side of the above equation is

$$\begin{aligned}
\sum_{\deg n \le N} \frac{\gamma^{\omega(n)}}{|n|} &= \prod_{\deg P \le N} \left(1 + \sum_{v=1}^{\infty} \frac{\gamma}{|P|^v}\right) \\
&\le \exp\left(\sum_{\deg P \le N} \sum_{v=1}^{\infty} \frac{\gamma}{q^{v \deg P}}\right) \\
&\ll \exp\left(\sum_{j=1}^{N} \sum_{v=1}^{\infty} \frac{q^j}{j} \cdot \frac{\gamma}{q^{vj}}\right) \\
&\ll \exp\left(\gamma \sum_{j=1}^{N} \frac{1}{j}\right) \\
&\ll N^{\gamma}.
\end{aligned}$$

Substituting this into (11.4) gives the lemma. □

The last calculation in the above proof will be useful later, and we record it as a lemma.

Lemma 11.6. *If $\gamma > 0$ and $N \ge 1$, then*

$$\sum_{\deg n \le N} \frac{\gamma^{\omega(n)}}{|n|} \ll N^{\gamma}.$$

11.3 Local solvability of homogeneous spaces

The problem of finding the sizes of the Selmer groups $Sel^{(\phi)}(E_n/K)$ is equivalent to the problem of determining the number of homogeneous spaces C_d having a non-trivial point over various local fields. The following lemma gives local solvability conditions for C_d.

Lemma 11.7. *Let $a, b \in R$ with $ab(a-b) \neq 0$ and $GCD(a,b) = 1$. Let $n \in R$ be a monic square-free polynomial with $GCD(n, ab(a-b)) = 1$, and let $M \subseteq K^*/K^{*2}$ be the multiplicative subgroup generated by a quadratic nonresidue α and all the primes dividing $(a-b)n$. Let P be a monic prime. For any $d \in M$, we have:*

1. *If $P|n$ and $P|d$, then $(\frac{ab}{P}) = 1$ and $(\frac{an/d}{P}) = 1 \iff C_d(K_P) \neq \mathbf{0}$.*
2. *If $P|n$ and $P \nmid d$, then $(\frac{d}{P}) = 1 \iff C_d(K_P) \neq \mathbf{0}$.*
3. *If $P|(a-b)$ and $P|d$, then $(\frac{-bn}{p}) = 1 \iff C_d(K_P) \neq \mathbf{0}$.*

4. *If* $\deg(a+b) = \deg(a-b)$ *and if* d *is a proper divisor of* $(a-b)n$ *with odd degree, then* $C_d(K_\infty) = \mathbf{0}$*, where* K_∞ *is the completion of* $K = \mathbb{F}_q(x)$ *with respect to the the prime* P_∞ *corresponding to the pole of* x*.*

Proof. Recall that

$$C_d : \qquad dw^2 = t^4 - 2(a+b)\frac{n}{d}t^2z^2 + (a-b)^2\frac{n^2}{d^2}z^4. \tag{11.5}$$

The first three cases are the function field analogue of [96, Lemma 6]. Let P be a finite prime, and v_P be its corresponding normalized valuation. If (w,t,z) is a non-trivial solution of (11.5), then so is (P^2w, Pt, Pz). Hence by multiplying a suitable power of P, we may assume that

$$\begin{aligned} 0 \leq \min\{v_P(w), v_P(t), v_P(z)\} \leq 1, \text{ and} \\ \min\{v_P(t), v_P(z)\} = 0 \text{ if } v_P(w) \geq 2. \end{aligned} \tag{11.6}$$

For case 1, let $P|n$ and $P|d$. From (11.5), the minimum of the 4 values

$$C_1 = 1 + 2v_P(w), \qquad C_2 = 4v_P(t), \qquad C_3 = v_P(a+b) + 2v_P(t) + 2v_P(z), \qquad C_4 = 4v_P(z),$$

is attained by at least two of them. With the assumptions (11.6) from the previous paragraph in mind, we have $C_2 = C_4 = 0$. Thus $v_P(t) = v_P(z) = 0$, but $C_1 > 0$ as it is odd. Hence

$$t^4 - 2(a+b)\frac{n}{d}t^2z^2 + (a-b)^2\frac{n^2}{d^2}z^4 \equiv 0 \pmod{P}.$$

Let $u = t/z \in (\mathcal{O}_P/P)^*$, then the above becomes

$$\left(u^2 - (a+b)\frac{n}{d}\right)^2 \equiv 4ab\frac{n^2}{d^2} \pmod{P}.$$

Hence we must have $(\frac{ab}{P}) = 1$. Let s be one of its square roots in $\mathcal{O}_P^*$, then

$$u^2 \equiv ((a+b) \pm 2s)\frac{n}{d} \pmod{P}.$$

So either $(\frac{(a+b+s)\frac{n}{d}}{P}) = 1$, or $(\frac{(a+b-s)\frac{n}{d}}{P}) = 1$. Since $(\frac{a}{P}) = (\frac{b}{P})$, a simple calculation reveals that we must have $(\frac{an/d}{P}) = 1$.

Conversely, if $(\frac{ab}{P}) = 1$ and $(\frac{an/d}{P}) = 1$, then by backtracking the above argument, we see that the

equation

$$t^4 - 2(a+b)\frac{n}{d}t^2z^2 + (a-b)^2\frac{n^2}{d^2}z^4 = 0$$

is solvable for $t \in (\mathcal{O}_P/P)^*$. By Hensel's lemma, this leads to a non-trivial solution $(0,t,1)$ of C_d over $\mathcal{O}_P^3$.

For case 2, let $P|n$, $P \nmid d$. Similar to the first case, with the assumptions (11.6) on the valuations for $v_P(w)$, $v_P(t)$ and $v_P(z)$, we have either

$$v_P(w) = v_P(t) = 0 \leq v_P(Z), \tag{11.7}$$

or

$$v_P(w) = 1, v_P(t) = 0, v_P(Z) \geq 1. \tag{11.8}$$

For (11.7), (11.5) gives $dw^2 \equiv t^4 \pmod{P}$, and so $(\frac{d}{P}) = 1$. For (11.8), we have

$$d\left(\frac{w}{P}\right)^2 \equiv (a-b)^2\frac{n^2}{p^2d^2}z^4 \pmod{P},$$

and again $(\frac{d}{P}) = 1$. Conversely, if $(\frac{d}{P}) = 1$, a similar argument as in the first case shows that one has a solution $(w,1,0) \in \mathcal{O}_P^3$.

For case 3, let $P|(a-b)$, $P|d$. Again with the assumptions (11.6) in mind and by considering the valuations, we obtain

$$1 + 2v_P(w) = -1 + 2v_P(t) + 2v_P(z) \text{ and } v_P(t) > 0.$$

The equation (11.5) becomes

$$\frac{d}{P}w^2 \equiv -2(a+b)\frac{np}{d}z^2 \pmod{P},$$

which implies $(\frac{-2(a+b)n}{P}) = 1$. Since $P|a-b$, this gives $(\frac{-bn}{P}) = 1$. The converse again follows from backtracking the arguments and using Hensel's lemma.

For case 4, let v_∞ be the normalized valuation at P_∞, thus $v_\infty(c) = -\deg(c)$ for $c \in R$. Suppose $t = 0$, then since $\deg d$ is odd, $v_\infty(dw^2)$ is odd but $v_\infty(2\frac{n^2}{d^2}z^4)$ is even. Thus there is no nontrivial solution of C_d with $t = 0$. Thus $t \neq 0$. Next, similar to the discussion in the paragraph before case 1, if (w,t,z) is a nontrivial solution of (11.5), then for any integer $j \neq 0$, $(x^{2j}w, x^jt, x^jz)$ is also one. Hence we may assume

that $\deg t = 0$. From the defining equation (11.5), the maximum of the four values

$$C_1 = \deg d + 2\deg w, \qquad C_2 = 0,$$
$$C_3 = \deg(a+b) + \deg n - \deg d + 2\deg z,$$
$$C_4 = 2\deg(a-b) + 2\deg n - 2\deg d + 4\deg z,$$

is attained by at least two of them. If $\deg(a+b) = \deg(a-b)$, then $C_4 = 2C_3$. As d is a proper divisor of $(a-b)n$, $C_3 \neq 0$. There are two cases, either $C_3 > 0$ or $C_3 < 0$. If $C_3 > 0$, then we must have $C_1 = C_4$. Note that C_1 is odd as $\deg d$ is odd, but $C_4 = 2C_3$ is even, so this is impossible. The case $C_3 < 0$ can be deal with similarly. This completes the proof. □

11.4 Averaging the size of Selmer groups $Sel^{(\phi)}(E_n/K)$

In this section we prove the following result, which will imply Theorem 11.1 immediately.

Lemma 11.8 (Function field analogue of Lemma 8 in [96]). *Let $a, b \in R$ with $ab(a-b) \neq 0$, $GCD(a,b) = 1$ and ab not a square. Let*

$$C_0 = \prod_{P \mid ab(a-b)} P,$$

and let $h, C \in R$ be coprime polynomials with $C_0 | C$. For any $N \geq 1$, let $S(N,h,C)$ be the set defined by (11.2), and for each $n \in S(N,h,C)$, let E_n be the elliptic curve over K defined by (11.1). Define $G \subseteq K^*/K^{*2}$ as the multiplicative subgroup generated by the prime divisors of n, and denote

$$\#(Sel^{(\phi)}(E_n/K) \cap G) = 2^{\hat{s}(n,\phi)}.$$

Then $\hat{s}(n,\phi) = 0$ for almost all $n \in S(N,h,C)$ as $N \to \infty$.

To see why Lemma 11.8 implies the theorem, note that from the definition of the Selmer group $Sel^{(\phi)}(E_n/K)$, we have

$$0 \leq s(n,\phi) \leq \hat{s}(n,\phi) + \omega(a-b) + 1,$$

and so

$$s(n,\phi) \leq \omega(a-b) + 1 \tag{11.9}$$

for almost all $n \in S(N,h,C)$ as $N \to \infty$. On the other hand, if $GCD(a,b) = c$ with $\deg c \geq 1$, then we may

rewrite E_n as

$$E_n : \qquad y^2 = x(x + a'n')(x + b'n'),$$

with $a = a'c$, $b = b'c$ and $n' = nc$. Lemma 11.8 is then applicable and we again obtain (11.9).

The proof of Lemma 11.8 is similar to that of [96, 97], in which the main idea is to bound the orders of Selmer groups using character sums. This idea was initially due to Heath-Brown [41, 42], and was generalized by Yu [98, 99, 100, 101]. Here we develop a function field analogue of their ideas.

To begin with, by Lemma 11.7, we have

$$2^{\hat{s}(n,\phi)} \leq \sum_{n=dd'} \prod_{P|d} \frac{1}{4} \left(\left(\frac{ab}{P} \right) + 1 \right) \left(\left(\frac{ad'}{P} \right) + 1 \right) \prod_{P|d'} \frac{1}{2} \left(\left(\frac{d}{P} \right) + 1 \right).$$

Expanding the product on the right hand side gives

$$\begin{aligned} 2^{\hat{s}(n,\phi)} \leq & \sum_{n=d_0d_1d_2d_3d_4d_5} 4^{-\omega(d_0d_1d_2d_3)} 2^{-\omega(d_4d_5)} \\ & \times \left(\frac{b}{d_1d_2} \right) \left(\frac{a}{d_2d_3} \right) \left(\frac{d_1}{d_4} \right) \left(\frac{d_4}{d_1} \right) \left(\frac{d_3}{d_4} \right) \left(\frac{d_4}{d_3} \right) \left(\frac{d_5}{d_1} \right) \left(\frac{d_5}{d_3} \right) \left(\frac{d_0}{d_4} \right) \left(\frac{d_2}{d_4} \right) \\ = & \sum_{n=d_0d_1d_2d_3d_4d_5} 4^{-\omega(d_0d_1d_2d_3)} 2^{-\omega(d_4d_5)} (-1)^{\frac{q-1}{2} \deg d_4 (\deg d_1 + \deg d_3)} \\ & \times \left(\frac{b}{d_1d_2} \right) \left(\frac{a}{d_2d_3} \right) \left(\frac{d_5}{d_1} \right) \left(\frac{d_5}{d_3} \right) \left(\frac{d_0}{d_4} \right) \left(\frac{d_2}{d_4} \right), \end{aligned}$$

where in the last step we used the quadratic reciprocity.

Let $\mathbf{d} = (d_0, d_1, d_2, d_3, d_4, d_5)$, the above sum is over all $\mathbf{d}$ with $n = d_0d_1d_2d_3d_4d_5$, d_i monic, squarefree and pairwise relatively prime. Denote by $g(\mathbf{d})$ the summand of the above sum. Our aim is to estimate the sum

$$\sum_{n \in S(N,h,C)} \sum_{\mathbf{d}} g(\mathbf{d}). \tag{11.10}$$

Let $D_i = \deg d_i$. The above sum is the same as summing all $\mathbf{d}$ with each d_i monic, squarefree and pairwise relatively prime, $\sum D_i = N$ and their product n satisfies the congruence $n \equiv h \pmod{C}$.

For a tuple of polynomials $\mathbf{d} = (d_0, d_1, \ldots, d_5)$, define

$$\deg(\mathbf{d}) = (\deg d_0, \deg d_1, \ldots, \deg d_5).$$

We divide the range of the sum (11.10) according to the degrees D_i of d_i. For any tuples

$$\mathbf{D} = (D_0, D_1, D_2, D_3, D_4, D_5)$$

with $\sum D_i = N$, we denote by $S(\mathbf{D})$ the subsum of (11.10) over all $\mathbf{d}$ with $\deg(\mathbf{d}) = \mathbf{D}$. There are $O(n^5)$ such subsums.

Following Heath-Brown [41, 42], we say two variables d_i and d_j are *linked* if exactly one of the quadratic characters

$$\left(\frac{d_i}{d_j}\right), \qquad \left(\frac{d_j}{d_i}\right)$$

appears in the expression for $g(\mathbf{d})$. Thus the pairs of linked variables are (d_1, d_5), (d_3, d_5), (d_0, d_4) and (d_2, d_4).

11.4.1 The first case

Consider the linked variables d_1, d_5. Suppose that both $D_1, D_5 \geq 1$, and $D_1 \geq D_5$. With the help of quadratic reciprocity, we can write $g(\mathbf{d})$ in the form

$$g(\mathbf{d}) = 4^{-\omega(D_1)} \left(\frac{d_1}{d_5}\right) \chi(d_1) c,$$

where χ is a (possibly trivial) character depending on d_1, and may also depend on other variables d_i. The number c satisfies $|c| < 1$, and is independent of d_1. We have

$$|S(\mathbf{D})| \leq \sum_{d_0, d_2, d_3, d_4, d_5} \left| \sum_{d_1} 4^{-\omega(d_1)} \left(\frac{d_1}{d_5}\right) \chi(d_1) \right|,$$

where d_1 is monic, squarefree, relatively prime to the other d_i's and satisfies $d_1 \equiv h' \pmod{C}$ for some h' determined by the congruence

$$n = d_0 d_1 d_2 d_3 d_4 d_5 \equiv h \pmod{C}.$$

The congruence condition above can be removed by inserting a factor

$$\frac{1}{\varphi(C)} \sum_{\psi \bmod C} \psi(d_1) \overline{\psi}(h').$$

After the congruence condition is removed, we may apply Lemma 11.4 to get

$$S(\mathbf{D}) \ll q^{N-(\frac{1}{2}-\varepsilon)D_1}.$$

Similar results hold when $D_5 \geq D_1$, and for other pairs of linked variables. We summarize the above calculations as follows.

Lemma 11.9. *We have*

$$S(\mathbf{D}) \ll q^{N-(\frac{1}{2}-\varepsilon)D}$$

whenever there is a pair of linked variables d_i, d_j such that $D_i, D_j \geq 1$ and $D = \max\{D_i, D_j\}$. In particular, if $D \geq \log_q^{11}(N)$, then

$$S(\mathbf{D}) \ll \frac{q^N}{N^{\frac{1}{2}}}. \tag{11.11}$$

11.4.2 The second case

In the rest of this chapter, all logarithms are to the base q unless otherwise stated. Suppose that exactly one of the D_4, $D_5 \leq \log^{11} N$, and at least three of the D_0, D_1, D_2, $D_3 \leq \log^{11} N$, but the conditions for (11.11) to hold in the first case are not met. Without loss of generality let $D_4 \leq \log^{11} N$, so that $D_5 \geq N/3$ is large and hence both $d_1 = 1$ (i.e. $D_1 = 0$) and $d_3 = 1$, or otherwise we are in the first case. Let $D_0 \leq \log^{11} N$.

Denote $\sum'$ be the sum over all $\mathbf{d}$ that satisfies the degree distribution under this situation. By using Lemma 11.5 and Lemma 11.6 several times, we obtain

$$\begin{aligned}
&\sum_{\mathbf{d}} |S(\mathbf{D})| \\
&\ll \sum_{\substack{d_0,d_4 \\ D_0,D_4 \leq \log^{11} N}} 4^{-\omega(d_0)} 2^{-\omega(d_4)} \sum_{\substack{d_2 \\ D_2 \leq N-D_0-D_4}} 4^{-\omega(d_2)} \sum_{\substack{d_5 \\ D_5 = N-D_0-D_2-D_4}} 2^{-\omega(d_5)} \\
&\ll \sum_{\substack{d_0,d_4 \\ D_0,D_4 \leq \log^{11} N}} 4^{-\omega(d_0)} 2^{-\omega(d_4)} \sum_{\substack{d_2 \\ D_2 \leq N-D_0-D_4}} 4^{-\omega(d_2)} \frac{q^N}{N^{\frac{1}{2}} q^{D_0} q^{D_2} q^{D_4}} \\
&\ll \frac{q^N}{N^{\frac{1}{2}}} \left(\sum_{\substack{d_0 \\ D_0 \leq \log^{11} N}} \frac{4^{-\omega d_0}}{|d_0|} \right) \left(\sum_{\substack{d_4 \\ D_4 \leq \log^{11} N}} \frac{2^{-\omega d_4}}{|d_4|} \right) \left(\sum_{\substack{d_2 \\ D_2 \leq N-D_0-D_4}} \frac{4^{-\omega d_2}}{|d_2|} \right) \\
&\ll \frac{q^N}{N^{\frac{1}{2}}} (\log^{11} N)(N^{\frac{1}{4}}) \\
&\ll \frac{q^N \log^{11} N}{N^{\frac{1}{4}}}.
\end{aligned}$$

Next, suppose that both D_4, $D_5 \leq \log^{11} N$, but one of d_4, $d_5 \neq 1$, say $d_4 \neq 1$, and the conditions for (11.11) are not met. In this case $d_5 = 1$ and D_0, $D_2 \leq \log^{11} N$. A similar calculation as above shows that the sum of $S(\mathbf{D})$ over all $\mathbf{d}$ in the current situation is $\ll \frac{q^N \log^{11} N}{N^{\frac{1}{4}}}$.

We summarize the results in the following lemma.

Lemma 11.10. *We have*

$$\sum_{\mathbf{D} \in T} |S(\mathbf{D})| \ll \frac{q^N \log^{11} N}{N^{\frac{1}{4}}},$$

where T is the set of all $\mathbf{D}$ such that either exactly one of D_4, $D_5 \leq \log^{11} N$ and at least three of D_0, D_1, D_2, $D_3 \leq \log^{11} N$, or both D_4, $D_5 \leq \log^{11} N$ but one of d_4, d_5 is not equal to 1.

11.4.3 The remaining cases

Suppose both D_4, $D_5 \geq \log^{11} N$. Then either we are in the first case, or $d_0 = d_1 = d_2 = d_3 = 1$. In the latter case we have $n = d_4 d_5$, and

$$g(\mathbf{d}) = 2^{-\omega(d_4)} 2^{-\omega(d_5)} = 2^{-\omega(n)}.$$

By Lemma 11.5, we can remove the condition on the size of D_4, D_5 with an error of at most

$$\sum_{\deg d_4 \leq \log^{11} N} \sum_{\deg d_5 \leq \log^{11} N} 2^{-\omega(d_4)} 2^{-\omega(d_5)} \ll q^{\log^{22} N}.$$

Since $n = d_4 d_5$ is squarefree, it factors as $d_4 d_5$ in exactly $2^{\omega(n)}$ distinct ways. Thus the sum of all contributions in this case is

$$\sum_{n \in S(N,h,C)} 1 + O(q^{\log^{22} N}) = \#S(N,h,C) + O(q^{\log^{22} N}). \tag{11.12}$$

Next, if $d_4 = d_5 = 1$, then

$$g(\mathbf{d}) = 4^{-\omega(n)} \left(\frac{b}{d_1}\right) \left(\frac{a}{d_3}\right) \left(\frac{ab}{d_2}\right).$$

If $D_2 \geq \log^{11} N$, then

$$S(\mathbf{D}) = \sum_{d_0, d_1, d_3} 4^{-\omega(d_0)} 4^{-\omega(d_1)} 4^{-\omega(d_3)} \left(\frac{b}{d_1}\right) \left(\frac{a}{d_3}\right) \sum_{\deg d_2 = D_2} 4^{-\omega(d_2)} \left(\frac{ab}{d_2}\right),$$

since $\deg ab \geq 1$ and ab is not a square in K, we can use Lemma 11.4 to bound the innermost sum. Thus we obtain

$$S(\mathbf{D}) \ll q^{N - D_2(\frac{1}{2} - \varepsilon)} \tag{11.13}$$

in this case. On the other hand, if $D_2 \leq \log^{11}(N)$, then a similar argument as the first part of the second case gives

$$\sum_{\mathbf{D}} |S(\mathbf{D})| \ll \frac{q^N \log^{11} N}{N^{\frac{1}{4}}}, \tag{11.14}$$

where the sum runs over all $\mathbf{D}$ that satisfies the current conditions.

11.4.4 Finishing the proof of Lemma 11.8

Combining Lemma 11.9, Lemma 11.10 and equations (11.12), (11.13), (11.14), we conclude that

$$\sum_{n \in S(N,h,C)} 2^{\hat{s}(n,\phi)} \leq \#S(N,h,C) + O\left(\frac{q^N \log^{11} N}{N^{\frac{1}{4}}}\right) \tag{11.15}$$

as $N \to \infty$.

For any integer $r \geq 0$, let

$$a_r = \#\{n \in S(N,h,C) : \hat{s}(n,\phi) = r\},$$

then (11.15) above becomes

$$\sum_{r \geq 0} 2^r a_r \leq \#S(N,h,C) + O\left(\frac{q^N \log^{11} N}{N^{\frac{1}{4}}}\right).$$

Thus

$$\sum_{r \geq 1} 2^{r-1} a_r \leq \sum_{r \geq 1} (2^r - 1) a_r = O\left(\frac{q^N \log^{11} N}{N^{\frac{1}{4}}}\right),$$

and hence we have

$$a_r = O\left(\frac{q^N \log^{11} N}{N^{\frac{1}{4}} 2^{-r}}\right) \ \forall r \geq 1,$$

and

$$\sum_{r \geq 1} a_r = O\left(\frac{q^N \log^{11} N}{N^{\frac{1}{4}}}\right).$$

Therefore, $\hat{s}(n,\phi) = 0$ for almost all $n \in S(N,h,C)$ as $N \to \infty$. This completes the proof of Lemma 11.8 and hence Theorem 11.1.

11.5 Further remarks

The argument presented in this chapter should also work on the dual isogeny $\hat{\phi} : E'_n \to E_n$ with

$$\hat{\phi}(X, Y) = \left(\frac{Y^2}{4X^2}, \frac{Y((a-b)^2 n^2 - X^2)}{8X^2} \right).$$

We expect that the resulting distribution of $Sel^{(\hat{\phi})}(E'_n/K)$ should be the same as in the number field case [97].

Conjecture 11.11. *Let*

$$Sel^{(\hat{\phi})}(E'_n/K) = 2^{s(n,\hat{\phi})},$$

then $s(n, \hat{\phi})$ follows a Gaussian distribution. More precisely, for any $\gamma \in \mathbb{R}$,

$$\lim_{N\to\infty} \frac{1}{\#S(N,h,C)} \# \left\{ n \in S(N,h,C) : \frac{s(n,\hat{\phi}) - \frac{1}{2}\log\log n}{\sqrt{\frac{1}{2}\log\log n}} \leq \gamma \right\} = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{\gamma} e^{\frac{-t^2}{2}}\, dt.$$

If we have a function field analogue of the result in [100], i.e. E_n has rank zero for most n, then the above conjecture together with Theorem 11.1 will yield information for the distribution of the Tate-Shafarevich groups $Ш(E_n/K)$.

On the other hand, it is also interesting to ask for the distribution of the Selmer groups in the characteristic 2 case (see Example 10.7), which bears no number field analogue. A descent process in this case can be found in [48]. However, since the behaviour of the Selmer group is different in characteristic 2, we do not know what kind of distribution to expect, or if the ideas from this chapter can be applied to that case as well.

References

[1] M. Abdón, J. Bezerra, and L. Quoos, *Further examples of maximal curves*, J. Pure Appl. Algebra **213** (2009), no. 6, 1192–1196.

[2] M. Abdón and F. Torres, *On maximal curves in characteristic two*, Manuscripta Math. **99** (1999), no. 1, 39–53.

[3] B. Angles and C. Maire, *A note on tamely ramified towers of global function fields*, Finite Fields Appl. **8** (2002), no. 2, 207–215.

[4] R. Auer, *Ray class fields of global function fields with many rational places*, Acta Arith. **95** (2000), no. 2, 97–122.

[5] A. Bassa, A. Garcia, and H. Stichtenoth, *A new tower over cubic finite fields*, Mosc. Math. J. **8** (2008), no. 3, 401–418, 615.

[6] J. Bezerra, A. Garcia, and H. Stichtenoth, *An explicit tower of function fields over cubic finite fields and Zink's lower bound*, J. Reine Angew. Math. **589** (2005), 159–199.

[7] E. Bombieri, *Counting points on curves over finite fields (d'après S. A. Stepanov)*, Séminaire Bourbaki, 25ème année (1972/1973), Exp. No. 430, Springer, Berlin, 1974, pp. 234–241. Lecture Notes in Math., Vol. 383.

[8] E. Çakçak and F. Özbudak, *Subfields of the function field of the Deligne-Lusztig curve of Ree type*, Acta Arith. **115** (2004), no. 2, 133–180.

[9] I. Cascudo, H. Chen, R. Cramer, and C.P. Xing, *Asymptotically good ideal linear secret sharing with strong multiplication over any fixed finite field*, Advances in cryptology—CRYPTO 2009, Lecture Notes in Comput. Sci., vol. 5677, Springer, Berlin, 2009, pp. 466–486.

[10] J. W. S. Cassels and A. Fröhlich, *Algebraic number theory*, London Mathematical Society, 2010.

[11] H. Chen and R. Cramer, *Algebraic geometric secret sharing schemes and secure multi-party computations over small fields*, Advances in cryptology—CRYPTO 2006, Lecture Notes in Comput. Sci., vol. 4117, Springer, Berlin, 2006, pp. 521–536.

[12] A. Cossidente, G. Korchmáros, and F. Torres, *On curves covered by the Hermitian curve*, J. Algebra **216** (1999), no. 1, 56–76.

[13] ———, *Curves of large genus covered by the Hermitian curve*, Comm. Algebra **28** (2000), no. 10, 4707–4728.

[14] P. Deligne and G. Lusztig, *Representations of reductive groups over finite fields*, Ann. of Math. (2) **103** (1976), no. 1, 103–161.

[15] V. G. Drinfel′d and S. G. Vlăduţ, *The number of points of an algebraic curve*, Funktsional. Anal. i Prilozhen. **17** (1983), no. 1, 68–69.

[16] I. Duursma and K.-H. Mak, *On lower bounds for the Ihara constants $A(2)$ and $A(3)$*, submitted, arXiv:1102.4127v3 [math.NT].

[17] ———, *On maximal curves which are not Galois subcovers of the Hermitian curve*, accepted for publication in Bull. Braz. Math. Soc. (N.S.), arXiv:1012.2068v3 [math.NT].

[18] S. Fanali and M. Giulietti, *Quotient curves of the GK curve*, ArXiv math.AG/0909.2582 (2009).

[19] G. Frey, M. Perret, and H. Stichtenoth, *On the different of abelian extensions of global fields*, Coding theory and algebraic geometry (Luminy, 1991), Lecture Notes in Math., vol. 1518, Springer, Berlin, 1992, pp. 26–32.

[20] R. Fuhrmann, A. Garcia, and F. Torres, *On maximal curves*, J. Number Theory **67** (1997), no. 1, 29–51.

[21] R. Fuhrmann and F. Torres, *The genus of curves over finite fields with many rational points*, Manuscripta Math. **89** (1996), no. 1, 103–106.

[22] A. Garcia, C. Güneri, and H. Stichtenoth, *A generalization of the Giulietti-Korchmáros maximal curve*, Adv. Geom. **10** (2010), no. 3, 427–434.

[23] A. Garcia and H. Stichtenoth, *A tower of Artin-Schreier extensions of function fields attaining the Drinfel′d-vlăduţ bound*, Invent. Math. **121** (1995), no. 1, 211–222.

[24] ———, *A maximal curve which is not a Galois subcover of the Hermitian curve*, Bull. Braz. Math. Soc. (N.S.) **37** (2006), no. 1, 139–152.

[25] A. Garcia, H. Stichtenoth, A. Bassa, and P. Beelen, *Towers of function fields over non-prime finite fields*, arXiv:1202.5922v1 [math.AG] (2012).

[26] A. Garcia, H. Stichtenoth, and C.P. Xing, *On subfields of the Hermitian function field*, Compositio Math. **120** (2000), no. 2, 137–170.

[27] W. Gaschütz and M. F. Newman, *On presentations of finite p-groups*, J. Reine Angew. Math. **245** (1970), 172–176.

[28] M. Giulietti, J. W. P. Hirschfeld, G. Korchmáros, and F. Torres, *Curves covered by the Hermitian curve*, Finite Fields Appl. **12** (2006), no. 4, 539–564.

[29] M. Giulietti and G. Korchmáros, *A new family of maximal curves over a finite field*, Math. Ann. **343** (2009), no. 1, 229–245.

[30] M. Giulietti, G. Korchmáros, and F. Torres, *Quotient curves of the Suzuki curve*, Acta Arith. **122** (2006), no. 3, 245–274.

[31] E. S. Golod and I. R. Shafarevich, *On the class field tower*, Izv. Akad. Nauk SSSR Ser. Mat. **28** (1964), 261–272.

[32] V. D. Goppa, *Geometry and codes*, Mathematics and its Applications (Soviet Series), vol. 24, Kluwer Academic Publishers Group, Dordrecht, 1988, Translated from the Russian by N. G. Shartse.

[33] C. Güneri, M. Özdemir, and H. Stichtenoth, *The automorphism group of the generalized giulietti-korchmaŕos function field*, To appear in Advances in Geometry.

[34] R. Guralnick, B. Malmskog, and R. Pries, *The automorphism groups of a family of maximal curves*, ArXiv math.NT/1105.3952 (2011).

[35] F. Hajir and C. Maire, *Asymptotically good towers of global fields*, European Congress of Mathematics, Vol. II (Barcelona, 2000), Progr. Math., vol. 202, Birkhäuser, Basel, 2001, pp. 207–218.

[36] ———, *Extensions of number fields with wild ramification of bounded depth*, Int. Math. Res. Not. (2002), no. 13, 667–696.

[37] R. R. Hall and G. Tenenbaum, *Divisors*, Cambridge Tracts in Mathematics, vol. 90, Cambridge University Press, Cambridge, 1988.

[38] J. P. Hansen, *Deligne-Lusztig varieties and group codes*, Coding theory and algebraic geometry (Luminy, 1991), Lecture Notes in Math., vol. 1518, Springer, Berlin, 1992, pp. 63–81.

[39] J. P. Hansen and J. P. Pedersen, *Automorphism groups of Ree type, Deligne-Lusztig curves and function fields*, J. Reine Angew. Math. **440** (1993), 99–109.

[40] R. Hartshorne, *Algebraic geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, No. 52.

[41] D. R. Heath-Brown, *The size of Selmer groups for the congruent number problem*, Invent. Math. **111** (1993), no. 1, 171–195.

[42] ———, *The size of Selmer groups for the congruent number problem. II*, Invent. Math. **118** (1994), no. 2, 331–370, With an appendix by P. Monsky.

[43] J. W. P. Hirschfeld, *Projective geometries over finite fields*, second ed., Oxford Mathematical Monographs, The Clarendon Press Oxford University Press, New York, 1998.

[44] K. Hoechsmann, *Zum Einbettungsproblem*, J. Reine Angew. Math. **229** (1968), 81–106.

[45] D. R. Hughes and F. C. Piper, *Projective planes*, Springer-Verlag, New York, 1973, Graduate Texts in Mathematics, Vol. 6.

[46] Y. Ihara, *Some remarks on the number of rational points of algebraic curves over finite fields*, J. Fac. Sci. Univ. Tokyo Sect. IA Math. **28** (1981), no. 3, 721–724.

[47] H. Koch, *Galois theory of p-extensions*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002, With a foreword by I. R. Shafarevich, Translated from the 1970 German original by Franz Lemmermeyer, With a postscript by the author and Lemmermeyer.

[48] K. Kramer, *Two-descent for elliptic curves in characteristic two*, Trans. Amer. Math. Soc. **232** (1977), 279–295.

[49] T. Kuhnt, *Generalizations of Golod-Shavarevich and applications*, Ph.D. thesis, University of Illinois at Urbana-Champaign, 2002.

[50] V. Landazuri and G. M. Seitz, *On the minimal degrees of projective representations of the finite Chevalley groups*, J. Algebra **32** (1974), 418–443.

[51] S. Lang, *Algebra*, third ed., Graduate Texts in Mathematics, vol. 211, Springer-Verlag, New York, 2002.

[52] S. Lang and A. Néron, *Rational points of abelian varieties over function fields*, Amer. J. Math. **81** (1959), 95–118.

[53] K. Lauter, *Deligne-Lusztig curves as ray class fields*, Manuscripta Math. **98** (1999), no. 1, 87–96.

[54] H. W. Lenstra, Jr., *On a problem of Garcia, Stichtenoth, and Thomas*, Finite Fields Appl. **8** (2002), no. 2, 166–170.

[55] M. Levin, *On the group of rational points on elliptic curves over function fields*, Amer. J. Math. **90** (1968), 456–462.

[56] W.-C. W. Li, *Upper and lower bounds for $A(q)$*, Recent trends in coding theory and its applications, AMS/IP Stud. Adv. Math., vol. 41, Amer. Math. Soc., Providence, RI, 2007, pp. 15–23.

[57] W.-C. W. Li and H. Maharaj, *Coverings of curves with asymptotically many rational points*, J. Number Theory **96** (2002), no. 2, 232–256.

[58] J. Neukirch, *Über das Einbettungsproblem der algebraischen Zahlentheorie*, Invent. Math. **21** (1973), 59–116.

[59] ———, *Algebraic number theory*, Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 322, Springer-Verlag, Berlin, 1999, Translated from the 1992 German original and with a note by Norbert Schappacher, With a foreword by G. Harder.

[60] J. Neukirch, A. Schmidt, and K. Wingberg, *Cohomology of number fields*, second ed., Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences], vol. 323, Springer-Verlag, Berlin, 2008.

[61] H. Niederreiter and C.P. Xing, *A construction of low-discrepancy sequences using global function fields*, Acta Arith. **73** (1995), no. 1, 87–102.

[62] ———, *Low-discrepancy sequences obtained from algebraic function fields over finite fields*, Acta Arith. **72** (1995), no. 3, 281–298.

[63] ———, *Low-discrepancy sequences and global function fields with many rational places*, Finite Fields Appl. **2** (1996), no. 3, 241–273.

[64] ———, *The algebraic-geometry approach to low-discrepancy sequences*, Monte Carlo and quasi-Monte Carlo methods 1996 (Salzburg), Lecture Notes in Statist., vol. 127, Springer, New York, 1998, pp. 139–160.

[65] ———, *Curve sequences with asymptotically many rational points*, Applications of curves over finite fields (Seattle, WA, 1997), Contemp. Math., vol. 245, Amer. Math. Soc., Providence, RI, 1999, pp. 3–14.

[66] ———, *Rational points on curves over finite fields: theory and applications*, London Mathematical Society Lecture Note Series, vol. 285, Cambridge University Press, Cambridge, 2001.

[67] ———, *Algebraic geometry in coding theory and cryptography*, Princeton University Press, Princeton, NJ, 2009.

[68] L. Ribes and P. Zalesskii, *Profinite groups*, second ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 40, Springer-Verlag, Berlin, 2010.

[69] M. Rosen, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002.

[70] H.-G. Rück and H. Stichtenoth, *A characterization of Hermitian function fields over finite fields*, J. Reine Angew. Math. **457** (1994), 185–188.

[71] R. Schoof, *Algebraic curves and coding theory*, UTM, vol. 336, University of Trento, 1990.

[72] ———, *Algebraic curves over* $\mathbf{F}_2$ *with many rational points*, J. Number Theory **41** (1992), no. 1, 6–14.

[73] J.-P. Serre, *Linear representations of finite groups*, Springer-Verlag, New York, 1977, Translated from the second French edition by Leonard L. Scott, Graduate Texts in Mathematics, Vol. 42.

[74] ———, *Local fields*, Graduate Texts in Mathematics, vol. 67, Springer-Verlag, New York, 1979, Translated from the French by Marvin Jay Greenberg.

[75] ———, *Rational points on curves over finite fields*, Lecture notes from a course taught at Harvard, 1985.

[76] ———, *Galois cohomology*, english ed., Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2002, Translated from the French by Patrick Ion and revised by the author.

[77] J. H. Silverman, *Advanced topics in the arithmetic of elliptic curves*, Graduate Texts in Mathematics, vol. 151, Springer-Verlag, New York, 1994.

[78] ———, *The arithmetic of elliptic curves*, second ed., Graduate Texts in Mathematics, vol. 106, Springer, Dordrecht, 2009.

[79] H. Stichtenoth, *Über die Automorphismengruppe eines algebraischen Funktionenkörpers von Primzahlcharakteristik. I, II*, Arch. Math. (Basel) **24** (1973), 527–544, 615–631.

[80] ———, *Algebraic function fields and codes*, second ed., Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009.

[81] H. Stichtenoth and C.P. Xing, *The genus of maximal function fields over finite fields*, Manuscripta Math. **86** (1995), no. 2, 217–224.

[82] K.-O. Stöhr and J. F. Voloch, *Weierstrass points and curves over finite fields*, Proc. London Math. Soc. (3) **52** (1986), no. 1, 1–19.

[83] J. Tate and I. R. Shafarevich, *The rank of elliptic curves*, Dokl. Akad. Nauk SSSR **175** (1967), 770–773.

[84] A. Temkine, *Hilbert class field towers of function fields over finite fields and lower bounds for $A(q)$*, J. Number Theory **87** (2001), no. 2, 189–210.

[85] M. A. Tsfasman and S. G. Vlăduţ, *Algebraic-geometric codes*, Mathematics and its Applications (Soviet Series), vol. 58, Kluwer Academic Publishers Group, Dordrecht, 1991, Translated from the Russian by the authors.

[86] M. A. Tsfasman, S. G. Vlăduţ, and Th. Zink, *Modular curves, Shimura curves, and Goppa codes, better than Varshamov-Gilbert bound*, Math. Nachr. **109** (1982), 21–28.

[87] D. L. Ulmer, *Park City lectures on elliptic curves over function fields*, `arXiv:1101.1939 [math.NT]`.

[88] ———, *p-descent in characteristic p*, Duke Math. J. **62** (1991), no. 2, 237–265.

[89] G. van der Geer and M. van der Vlugt, *An asymptotically good tower of curves over the field with eight elements*, Bull. London Math. Soc. **34** (2002), no. 3, 291–300.

[90] J. H. van Lint and G. van der Geer, *Introduction to coding theory and algebraic geometry*, DMV Seminar, vol. 12, Birkhäuser Verlag, Basel, 1988.

[91] J. F. Voloch, *Explicit p-descent for elliptic curves in characteristic p*, Compositio Math. **74** (1990), no. 3, 247–258.

[92] C. A. Weibel, *An introduction to homological algebra*, Cambridge Studies in Advanced Mathematics, vol. 38, Cambridge University Press, Cambridge, 1994.

[93] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945), Hermann et Cie., Paris, 1948.

[94] ———, *Variétés abéliennes et courbes algébriques*, Actualités Sci. Ind., no. 1064 = Publ. Inst. Math. Univ. Strasbourg 8 (1946), Hermann & Cie., Paris, 1948.

[95] C.P. Xing and S. L. Yeo, *Algebraic curves with many points over the binary field*, J. Algebra **311** (2007), no. 2, 775–780.

[96] M. Xiong and A. Zaharescu, *Distribution of Selmer groups of quadratic twists of a family of elliptic curves*, Adv. Math. **219** (2008), no. 2, 523–553.

[97] ———, *Selmer groups and Tate-Shafarevich groups for the congruent number problem*, Comment. Math. Helv. **84** (2009), no. 1, 21–56.

[98] G. Yu, *Rank 0 quadratic twists of a family of elliptic curves*, Compositio Math. **135** (2003), no. 3, 331–356.

[99] ———, *Average size of 2-Selmer groups of elliptic curves. II*, Acta Arith. **117** (2005), no. 1, 1–33.

[100] ———, *On the quadratic twists of a family of elliptic curves*, Mathematika **52** (2005), no. 1-2, 139–154 (2006).

[101] ———, *Average size of 2-Selmer groups of elliptic curves. I*, Trans. Amer. Math. Soc. **358** (2006), no. 4, 1563–1584 (electronic).

[102] Th. Zink, *Degeneration of Shimura surfaces and a problem in coding theory*, Fundamentals of computation theory (Cottbus, 1985), Lecture Notes in Comput. Sci., vol. 199, Springer, Berlin, 1985, pp. 503–511.